UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Tomaž Paternoster

Transformacija sporočil sistema kratkih sporočil (SMS) v digitalno podpisana in časovno overovljena sporočila XML

DIPLOMSKO DELO

DIPLOMSKO DELO NA UNIVERZITETNEM ŠTUDIJU

Breg pri Litiji, 2016

UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Tomaž Paternoster

Transformacija sporočil sistema kratkih sporočil (SMS) v digitalno podpisana in časovno overovljena sporočila XML

DIPLOMSKO DELO

DIPLOMSKO DELO NA UNIVERZITETNEM ŠTUDIJU

MENTOR: prof. dr. Denis Trček

Breg pri Litiji, 2016

To delo je ponujeno pod licenco *Creative Commons Priznanje avtorstva-Deljenje pod enakimi pogoji 2.5 Slovenija* (ali novejšo različico). To pomeni, da se tako besedilo, slike, grafi in druge sestavine dela kot tudi rezultati diplomskega dela lahko prosto distribuirajo, reproducirajo, uporabljajo, priobčujejo javnosti in predelujejo, pod pogojem, da se jasno in vidno navede avtorja in naslov tega dela in da se v primeru spremembe, preoblikovanja ali uporabe tega dela v svojem delu, lahko distribuira predelava le pod licenco, ki je enaka tej. Podrobnosti licence so dostopne na spletni strani creativecommons.si ali na Inštitutu za intelektualno lastnino, Streliška 1, 1000 Ljubljana.

Izvorna koda diplomskega dela, njeni rezultati in v ta namen razvita programska oprema je ponujena pod licenco *GNU General Public License*, različica 3 (ali novejša). To pomeni, da se lahko prosto distribuira in/ali predeluje pod njenimi pogoji. Podrobnosti licence so dostopne na spletni strani http://www.gnu.org/licenses.

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Tematika naloge:

V diplomskem delu proučite in implementirajte možnosti izvajanja sprememb v naročniških razmerjih pri mobilnih operaterjih preko sporočil SMS. Upoštevajte trenutno obstoječo slovensko zakonodajo in priporočila na področju elektronskega podpisa in elektronskega arhiviranja. Izdelajte programsko rešitev za pretvorbo in hranjenje sporočil SMS, opišite uporabljena programska orodja, posamezne korake pri izdelavi rešitve in postopke testiranja.

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Spodaj podpisani Tomaž Paternoster sem avtor diplomskega dela z naslovom:

Transformacija sporočil sistema kratkih sporočil (SMS) v digitalno podpisana in časovno overovljena sporočila XML (angl. Transformation of short message service (SMS) messages into digitally signed and time-certified XML messages)

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom prof. dr. Denisa Trčka,
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela,
- soglašam z javno objavo elektronske oblike diplomskega dela na svetovnem spletu preko univerzitetnega spletnega arhiva.

Na Bregu pri Litiji, dne 25. marca 2016 Podpis avtorja:

Zahvaljujem se prof. Dr. Denisu Trčku za strokovno pomoč in usmerjanje pri pripravi diplomske naloge. Prav tako se zahvaljujem svoji družini za vso moralno podporo in spodbudo pri dokončanju študija. Posebna zahvala pa gre vsem, ki so verjeli, da nisem obupal.

Kazalo

Seznam uporabljenih kratic

kratica	angleško	slovensko
API	Application Programming Interface	Aplikativni programski vmesniki
AS 1/2/3/4	Applicability Statement 1/2/3/4	Standardi za elektronsko poslovanje
B2B	Business to Business	Izmenjava sporočil v skladu s standardom izmenjave sporočil med partnerji
COBOL	Common Business Oriented Language	Prvotno nestrukturiran programski jezik
CPPA	ebXML Collaboration Protocol Profile Agreement	Standard za elektronsko poslovanje
CSR	Certificate Signing Request	Zahtevek za pridobitev digitalnega potrdila
DoS	Denial of Service	Ohromitev storitve
ebXML	Electronic Business XML	Razširljivi označevalni jezik za elektronsko poslovanje
EDI	Electronic data interchange	Standard za elektronsko poslovanje
ESB	Enterprise Service Bus	Visoko zmogljivo storitveno vodilo
ESX	Vmware Hypervisor product	Hipervizor podjetja VMware
ETSI	European Telecommunications Standards Institute	Evropski inštitut za telekomunikacijske standarde
FIPS	Federal Information Processing Standards	Standardi za kriptografske module
FTP	File Transfer Protocol	Protokol za prenos datotek
GSM	Global System for Mobile	Globalni sistem za mobilne

	Communications	komunikacije
HL7	Health Level Seven	Nabor mednarodnih standardov za izmenjavo zdravstvenih podatkov
HTTP	Hyper Text Transfer Protocol	Protokol za prenos hiperteksta
ID	Identification number	Enolični identifikator
IETF	Internet Engineering Task Force	Glavna organizacija za tehnični razvoj in standard interneta
IP	Internet Protocol	Internetni protokol
JMS	Java Message Service	Storitev za asinhrono izmenjavo podatkov
MQ	Message Queue	Vmesna programska oprema za asinhrono izmenjavo podatkov
MSISDN	Mobile Station International Subscriber Directory Number	Nacionalna značilna številka, ki jo mobilnemu uporabniku dodeli operater
NTP	Network Time Protocol	Omrežni časovni protokol
PDF	Portable Document Format	Oblika zapisa sporočil
PKCS7	Cryptographic Message Syntax Standard	Kriptografski standard za sintakso sporočil
PKI	Public Key Infrastructure	Infrastruktura javnega ključa
POP3	Post Office Protocol 3	Standard za prejemanje elektronske pošte
RFC#	Request for Comments #	Tip publikacije organizacije IETF
RSA	Rivest-Shamir-Adleman cryptosystem	Kriptografski algoritem
SEPA	Single Euro Payments Area	Iniciativa Evropske Unije za elektronsko integracijo plačil
SMS	Short Message Service	Sistem kratkih sporočil
SMS-SC	Short Message Service – Service Center	Storitveni center za sistem kraktih sporočil
SMTP	Simple Mail Transfer Protocol	Standard za prenos elektronske pošte
SOA	Service Oriented Architecture	Storitveno usmerjena arhitektura

SOAP	Simple Object Access Protocol	Protokol za spletne storitve
SQL	Structured Query Language	Strukturiran povpraševalni jezik
SSL	Secure Sockets Layer	Kriptografski protokol za zaščito komunikacij
SWIFT	Society for Worldwide Interbank Financial Telecommunication	Združenje za standardizacijo medbančnih finančnih telekomunikacij
TLS	Transport Layer Security	Kriptografski protokol za zaščito komunikacij
TSA	Time Stamp Authority	Zupanja vredna avtoriteta za časovno žigosanje
URI	Uniform Resource Identifier	Enolični označevalnik vira
URL	Unfiorm Resource Locator	Enolični krajevnik vira
WSDL	Web Service Definition Language	Jezik za opis spletnih storitev
WS-Sec	Web Service Security	Protokol za zaščito spletnih storitev
XML	Extensible Markup Language	Razširljivi označevalni jezik
XSL	Extensible Stylesheet Language	Družina jezikov za oblikovanje, preoblikovanje in prikazovanje XML
XSLT	Extensible Stylesheet Language Transformations	Transformacije za XSL

Povzetek

Naslov: Transformacija sporočil sistema kratkih sporočil (SMS) v digitalno podpisana in časovno overovljena sporočila XML

V diplomskem delu predstavimo idejo za izvajanje sprememb v naročniških razmerjih pri mobilnih operaterjih preko sporočil SMS. Pregledamo in predstavimo povzetek trenutno obstoječe slovenske zakonodaje in priporočil na področju elektronskega podpisa in elektronskega arhiviranja. Sledeč ugotovljenim priporočilom in zakonom izdelamo programsko rešitev za pretvorbo in hranjenje sporočil SMS, opišemo uporabljena programska orodja, posamezne korake pri izdelavi rešitve in postopke testiranja. Opišemo ključna področja in smernice, ki se jih moramo pri izdelavi programske rešitve držati. V zaključku podamo usmeritev, kako lahko idejo uporabimo v praksi in tekom razvoja ugotovljene izboljšave izdelane rešitve.

Ključne besede: sporočilo SMS, sporočilo XML, e-arhiviranje, transformacija sporočil, naprava DataPower, SMS Gateway aplikacija, digitalni podpis, časovni žig

Abstract

Title: Transformation of short message service (SMS) messages into digitally signed and time-certified XML messages

Thesis describes the idea of changing customer mobile subscription via SMS messages. We review and present a summary of Slovenian legislation for digital signature and electronic archiving. Following identified recommendations and laws we prepare software solution for transformation and archiving of SMS messages, describe software tools we used, steps in creation of software solution and testing procedures. We describe key areas and guidelines that we need to follow during preparation of software solution, we conclude with giving directions to practical use of implemented idea and identified improvements of software solution.

Keywords: SMS message, XML message, e-archiving, message transformation, DataPower appliance, SMS Gateway application, digital signature, timestamp

Poglavje 1 Uvod

1.1 Opis problema

Prvo sporočilo SMS je bilo poslano v začetku decembra daljnega leta 1992, ko je Neil Papworth, kanadski računalniški inženir za podjetje Sema Group, poslal preprosto kratko sporočilo (»Merry Christmas«) s svojega računalnika na mobilni telefon v omrežju Vodafone. Sprva so sistem kratkih sporočil SMS uporabljali zgolj za omrežna obvestila (na primer obvestilo o čakajočem glasovnem sporočilu), v letu 1993 pa je podjetje Nokia ponudilo prvo mobilno napravo, ki je uporabnikom omogočala pošiljanje sporočil SMS.

Danes je sistem kratkih sporočil SMS eden izmed najbolj popularnih in razširjenih načinov komuniciranja. Po nekaterih podatkih naj bi ga aktivno uporabljalo več kot 3.5 milijarde uporabnikov oziroma okoli 80% vseh uporabnikov mobilnih telefonov (povzeto po [20]).

Povečano uporabo takšnega sistema so prepoznali tudi mobilni operaterji, ki so uporabnikom ponudili vklop različnih storitev preko sporočil SMS. Primer takšne storitve je recimo vklop zgrešenih klicev ali zakup prenosa podatkov. Takšno storitev uporabnik naroči s poslanim sporočilom SMS z ustrezno ključno besedo na določeno telefonsko številko pri mobilnem operaterju.

Na trgu mobilnih komunikacijskih storitev se v zadnjih letih izkazuje potreba in želja uporabnikov po vse več mobilnih storitvah, ki bi jih lahko uporabljali s sporočili SMS, med drugim tudi storitve, za katere mobilni operaterji potrebujejo naročnikov lastnoročni podpis pogodbe ali aneksa. Za takšne storitve mora naročnik obiskati poslovni center mobilnega operaterja, se pogovoriti z referentom in skleniti spremembo naročniškega razmerja. Kljub temu, da so danes takšne spremembe hitre (predvsem s stališča tehnične izvedbe) pa naročniku še vedno vzamejo kar nekaj časa.

V računalniškem svetu se je za potrebe izkazovanja identitete uporabnika in integritete sporočila uveljavila tehnologija elektronskih podpisov, in sicer predvsem digitalnega podpisa. Slovenska zakonodaja predpisuje, da je digitalni podpis pod določenimi pogoji enakovreden lastnoročnemu. Težave nastane pri uporabi digitalnega podpisa s sistemom kratkih sporočil SMS, ki niso zasnovana za takšno uporabo.

V diplomski nalogi smo razvili sistem, ki naslavlja opisan problem in ga delno tudi odpravlja. Razviti sistem bi mobilni operaterji lahko uporabili za pospešitev poslovnih procesov in s prihrankom časa ter hitrejšo aktivacijo storitev tudi večje zadovoljstvo naročnikov.

1.2 Cilj diplomskega dela

Željo trga po upravljanju mobilnih naročniških razmerij preko sistema kratkih sporočil SMS lahko delno rešimo brez spreminjanja obstoječe tehnologije. Zamislimo si sistem, kjer lahko naročnik pošlje sporočilo SMS z željenimi spremembami naročniškega razmerja (vklop/izklop storitev, sprememba naročniškega paketa, zakup novih storitev ...), mobilni operater pa prejeto sporočilo SMS obravnava kot pravno podlago za aktivacijo željenih sprememb in naročniku v podpis posreduje spremembo pogodbe ali aneks k obstoječemu naročniškemu razmerju.

Cilj diplomske naloge je izdelati sistem, ki bi omogočil trajno shranjevanje sporočil SMS v obliki digitalno podpisanih in časovno overovljenih sporočil XML, na podlagi katerih bi lahko mobilni operaterji izvajali spremembe naročniških razmerij in aktivacije oz. deaktivacije storitev, za katere se v njihovem poslovnem procesu sicer potrebuje lastnoročni podpis naročnika.

V diplomski nalogi bomo preučili trenutno veljavno zakonodajo na področju digitalnega podpisa in na podlagi pridobljenih informacij izdelali testni sistem za transformacijo sporočil sistema kratkih sporočil v digitalno podpisano in časovno overovljeno sporočilo XML, ki bo po trenutno veljavni slovenski zakonodaji prepoznano kot pravno veljaven dokument. Rešitev bo nadalje skladna s tehnološkimi standardi na področju e-arhiviranja in bo sledila priporočilom dokumentacije e-SLOG.

Sistem bomo izdelali s pomočjo komercialnih orodij podjetja IBM, mobilne naprave z operacijskim sistemom Android ter odprtokodne in prosto dostopne programske opreme:

- IBM Transformation Extender,
- IBM DataPower Gateway,
- SoapUI,
- cURL,
- OpenSSL,
- SMS Gateway,
- Android mobilna naprava

Za izmenjavo bomo uporabili nabor podatkov, za katere predvidevamo, da bi jih mobilni operaterji potrebovali v svojem poslovnem procesu in na podlagi katerih bi lahko izvajali željene spremembe v naročniških razmerjih.

Poglavje 2 Pregled zakonodaje in priporočil na področju elektronskega podpisa

V Sloveniji področje elektronskega podpisa ureja Zakon o elektronskem poslovanju in elektronskem podpisu s pripadajočo Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje, področje elektronskega arhiviranja dokumentov pa Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih s pripadajočo Uredbo o varstvu dokumentarnega in arhivskega gradiva.

V predpisih na področju Republike Slovenije področje sintakse in procesiranja XML digitalnega podpisa ni posebej urejeno, zato imamo za omenjena področja še priporočila (vsebinska in tehnična), ki naj bi jim sledili za zagotavljanje enotnega načina uporabe elektronskega podpisa.

Gospodarska Zbornica Slovenije je v letih od 2001 do 2006 izvajala projekt e-SLOG, v katerem so želeli povezati interese in strokovnjake iz več podjetij in jih združiti pri pripravi in uveljavljanju enotnih slovenskih priporočil za elektronske dokumente in tehnološko povezovanje podjetij. Priporočila so bila potrebna predvsem na področju elektronskega poslovanja, za poslovne dokumente, kot so naročilnica, dobavnica in račun. V okviru delovne skupine za elektronski podpis so na podlagi mednarodnih standardov in priporočil nastala priporočila za format dokumenta XML za varen e-podpis in priporočila za uporabo kriptografskih algoritmov.

V okviru projekta e-SLOG nastajajo tudi Tehnična priporočila za varno elektronsko arhiviranje.

2.1 Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA)

Zakon ZVDAGA in pripadajočo uredbo smo preverili, da bi pridobili informacije o tem, kaj je elektronsko gradivo, kakšna je dokazna vrednost takega gradiva in na kakšen način ter pod

katerimi pogoji ga moramo hraniti. Še posebej nas zanima, kako je opredeljena pretvorba elektronskega gradiva in kaj moramo ob tem zagotoviti.

V uvodnih določbah prvi člen zakona podaja opis in namen.

»Ta zakon ureja način, organizacijo, infrastrukturo in izvedbo zajema ter hrambe dokumentarnega gradiva v fizični in elektronski obliki, veljavnost oziroma dokazno vrednost takega gradiva, varstvo arhivskega gradiva in pogoje za njegovo uporabo, naloge arhivov in javne arhivske službe ter s tem povezane storitve in nadzor nad izvajanjem. «[1]

Zanima nas predvsem, kako zakon opredeljuje elektronske dokumente in njihovo hrambo v elektronski obliki.

Zakon opredeljuje pojem elektronski dokument kot dokumentarno gradivo v digitalni obliki, shranjeno na elektronskem nosilcu, ki je bilo prejeto ali je nastalo pri delu pravnih oziroma fizičnih oseb. Obliko zapisa elektronskega dokumenta opredeljuje z organizacijskimi in tehnološkimi značilnostmi, ki določajo, kako je vsebina zapisana, hranjena in prikazana v procesu hrambe. Hrambo elektronskih dokumentov pa zakon opredeljuje kot hrambo dokumentarnega gradiva, ki izpolnjuje pogoje po tem zakonu in zagotavlja uporabnost vsebine hranjenega gradiva.

Opredeljuje tudi strojno in programsko opremo za hrambo gradiva v digitalni obliki, in sicer kot vsako strojno oziroma programsko opremo, katere namen je v celoti ali delno omogočiti zajem in hrambo gradiva v digitalni obliki ter s tem povezana opravila. Zagotavljati mora varnost gradiva pred uničenjem, neprekinjeno poslovanje, varnost dostopa, prepis oziroma pretvorbo gradiva, ohranjanje dokazljivosti avtentičnosti in celovitosti, evidentiranje vseh dogodkov med hrambo oziroma v zvezi s hrambo gradiva (71.člen).

V načelu trajnosti (4.člen), načelu celovitosti (5.člen) in načelu dostopnosti (6.člen) je določeno, da mora hramba elektronskega gradiva zagotavljati trajnost oziroma trajnost reprodukcije vsebine elektronskega dokumenta, njegovo nespremenljivost in integralnost ter dokazljivost izvora. Hkrati mora biti vsebina elektronskega dokumenta ves čas trajanja hrambe zavarovana pred izgubo ali okrnitvijo celovitosti ter dostopna pooblaščenim uporabnikom (26.člen).

Oblika elektronskega zapisa mora zagotavljati ohranitev vsebine gradiva več kot pet let ter omogočati po tem obdobju pretvorbo v novo digitalno obliko zapisa, ki bo takrat izpolnjevala pogoje varne hrambe gradiva (29.člen). Nosilec zapisa mora zagotavljati vse pogoje varne

hrambe gradiva in omogočati večje število prepisov s sedanjih na bodoče nosilce zapisa (30.člen).

Pripadajoča uredba zakona med drugim opredeljuje informacijski sistem za hrambo kot informacijski sistem za skladiščenje in iskanje elektronskega gradiva, ki nadzoruje posebne funkcije nastajanja, hrambe in dostopa do gradiva zato, da ohranjajo njegovo uporabnost, celovitost in dostopnost (2.člen).

Pretvorba elektronskega gradiva iz ene oblike v drugo obliko mora omogočati pravilno pretvorbo vseh ključnih vsebinskih podatkov in metapodatkov, ustvariti vse potrebne metapodatke glede pretvorbe (dodatni podatki o avtentičnosti gradiva, datum pretvorbe, postopek pretvorbe ...) in zagotoviti uporabnost vsebine gradiva. Omogočati mora samodejno in ročno pravilnost pretvorbe vsebine in metapodatkov, varnost in nespremenljivost pretvorjenega elektronskega gradiva po pravilni pretvorbi ter poznejše popravke napak pri pretvorbi in upravičeno dopolnjevanje metapodatkov samo s strani pooblaščenih oseb in z zagotavljanjem jasne revizijske sledi takšnih popravkov ali dopolnitev (13.člen).

Avtentičnost in celovitost zajetega elektronskega gradiva mora biti zagotovljena ves čas hrambe gradiva. Zagotavlja se z dodajanjem varnostnih vsebin gradivu, kot so elektronski podpis, časovni žig in podobno (17.člen).

Strojna in programska oprema za zajem in hrambo elektronskega gradiva mora biti široko priznana in uveljavljena oziroma uporabljana ali posebej razvita za zajem in hrambo gradiva v digitalni obliki. Mora biti skladna z mednarodnimi, državnimi in drugimi splošno priznanimi standardi, z določbami zakona, uredbe in enotnimi tehnološkimi zahtevami (19. in 20.člen).

Ponudnik storitve hranjenja elektronskih dokumentov mora podatke varovati kot dober strokovnjak in v skladu z uveljavljenimi pravili stroke. Prostori in infrastruktura morajo biti ustrezno elektronsko in fizično varovani, dostopi do prostorov in opreme, tako strojne kot programske, morajo biti nadzorovani in evidentirani. Informacijsko-komunikacijska infrastruktura mora biti varovana z zanesljivimi varnostnimi mehanizmi (požarne pregrade, sistemi za preprečevanje vdorov ...), ki preprečujejo nepooblaščene dostope ali vdore (22.člen).

Zakon in Uredba sta v veljavi od leta 2006 (povzeto po [1,2]).

2.2 Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP)

Po pregledu in pojasnilu, kaj je elektronsko gradivo in na kakšen način ga je potrebno hraniti, moramo preučiti še konkretnejše področje elektronskega podpisa. Zanima nas, kako so opredeljeni elektronski podatki, elektronski podpis in časovni žig ter na kakšen način jih lahko zagotovimo in uporabljamo. Nadalje moramo preučiti, pod katerimi pogoji je prepoznan izvor, čas prejema in oblika hrambe elektronskega sporočila ter pod katerimi pogoji so elektronski podatki enakovredni pisnim.

Zakon o elektronskem poslovanju in elektronskem podpisu ureja poslovanje v elektronski obliki z uporabo informacijskih in komunikacijskih tehnologij in uporabo elektronskega podpisa v pravnem prometu (1.člen).

Podatki v elektronski obliki so podatki, oblikovani, poslani, prejeti ali izmenljivi na elektronski način.

Elektronski podpis je opredeljen kot niz elektronskih podatkov, ki je vsebovan, dodan ali logično povezan z drugimi podatki, in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika.

Časovni žig je elektronsko podpisano potrdilo overitelja in potrjuje vsebino podatkov, na katere se nanaša, v navedenem času.

Zakon opredeljuje tudi sredstva in podatke za elektronsko podpisovanje. Sredstva so opredeljena kot nastavljena programska ali strojna oprema, ki se uporablja za oblikovanje elektronskega podpisa, podatki pa kot edinstveni podatki, kot so šifre ali šifrirni ključi, ki jih podpisnik uporablja za podpisovanje elektronskega dokumenta. Oprema za elektronsko podpisovanje je strojna ali programska oprema, ki jo overitelj uporablja za storitve v zvezi z elektronskim podpisovanjem (2.člen).

Zakon predpisuje, da elektronsko sporočilo izvira od pošiljatelja, če ga pošlje pošiljatelj sam ali v njegovem imenu oseba, pooblaščena s strani pošiljatelja, in če je naslovnik za potrditev izvora sporočila uporabil dogovorjeno tehnologijo in postopek. Pošiljatelj lahko prejemnika obvesti, da sporočilo ni njegovo oziroma lahko prejemnik kot dober gospodar ugotovi, da sporočilo ni pošiljateljevo (5.člen).

Elektronsko sporočilo se šteje za prejeto, če prejemnik o prejemu sporočila v razumnem časovnem roku obvesti pošiljatelja ali izvede kakršno koli aktivnost, ki zadostuje, da

pošiljatelj izve, da je bilo elektronsko sporočilo prejeto. Slednje velja v primeru, da ni dogovora o obliki potrdila o prejemu sporočila (7.člen).

Za čas prejema elektronskega sporočila se šteje trenutek vstopa sporočila v prejemnikov informacijski sistem (10.člen).

Podatki se lahko v elektronski obliki hranijo, če so vsebovani v elektronskem dokumentu, dosegljivi in primerni za kasnejšo uporabo, shranjeni v originalni obliki ali v obliki, ki jih verodostojno predstavlja. Mogoče mora biti ugotoviti njihov izvor, ponor, čas in kraj pošiljanja ter prejema (12.člen).

Elektronska oblika je enakovredna pisni, če so podatki v elektronski obliki dosegljivi in primerni za kasnejšo uporabo (13.člen).

Zakon zapoveduje, da je varen elektronski podpis, overjen s kvalificiranim potrdilom, enakovreden lastnoročnemu podpisu ter ima zato enako veljavnost in dokazno vrednost (15.člen). Zapoveduje tudi, da morajo osebe, ki hranijo elektronsko podpisane dokumente, enako dolgo hraniti tudi komplementarne podatke in sredstva za preverjanje elektronskega podpisa (16.člen).

Sredstva za elektronsko podpisovanje morajo zagotavljati edinstvene, zaupanja vredne podatke za elektronsko podpisovanje in jih ne smejo spreminjati. Teh podatkov v razumnem času in z razumnimi sredstvi tudi ne sme biti mogoče ugotoviti iz podatkov za preverjanje elektronskega podpisa (37.člen).

Preverjanje elektronskega podpisa mora biti izvedeno z uporabo ustreznih podatkov in ustrezno infrastrukturo. Podpis mora biti zanesljivo preverjen in rezultati preverjanja ter identiteta podpisnika pravilno prikazana. Pristnost in veljavnost potrdila morata biti preverjeni v času preverjanja podpisa (38.člen).

Zakonu pripadajoča uredba med drugim določa podrobnejše tehnične pogoje za elektronsko podpisovanje in preverjanje varnih elektronskih podpisov, časovno veljavnost kvalificiranih potrdil ter podrobnejše pogoje glede uporabe varnih časovnih žigov (1.člen).

Uporaba podatkov za varno elektronsko podpisovanje mora zahtevati zavestno in zanesljivo dejanje za predstavitev sredstev za varno elektronsko podpisovanje (na primer vnos gesla) razen v primeru, ko gre za samodejno odzivanje informacijskega sistema (25.člen).

Sredstvo za preverjanje varnega elektronskega podpisa mora uporabniku omogočati, da jasno ugotovi, kateri podatki in v kakšnem obsegu so bili podpisani. Uporabnik mora tudi vedno

preveriti veljavnost potrdila v skladu z navodili overitelja, še posebej, če je potrdilo navedeno v registru preklicanih potrdil (26.člen).

Časovna veljavnost kvalificiranih potrdil, razen lastnega kvalificiranega potrdila overitelja, je največ pet let od izdaje (32.člen).

Varen časovni žig mora biti najmanj na sekundo natančen. Vsebovati mora točen čas in datum ter podatke o overitelju, ki je varni časovni žig ustvaril. Dokumentu je lahko dodan, priložen ali z njim povezan (34.člen). Informacijski sistem, ki izdaja varen časovni žig, mora biti sinhroniziran z virom točnega časa (35.člen).

Zakon in Uredba sta v veljavi od leta 2000 in do danes nista doživela večjih sprememb (povzeto po [3,4]).

2.3 e-SLOG dokumentacija

Rezultat projekta e-SLOG je skupek dokumentacije, navodil in priporočil za uporabo elektronskega podpisa v poslovanju. Zanimajo nas predvsem priporočila za format dokumenta XML za varen e-podpis, priporočila uporabe kriptografskih algoritmov in tehnična priporočila za varno elektronsko arhiviranje.

Delovna skupina za e-podpis se v priporočilih opira na standarde in priporočila mednarodne organizacije W3C (World Wide Web Consortium), katere poslanstvo je razvoj tehnologij in standardov za povezljivost aplikacij v spletnem okolju, in neprofitne organizacije ETSI (European Telecommunications Standards Institute), katere poslanstvo je priprava standardov in smernic razvoja telekomunikacijskih storitev in informacijske tehnologije za področje Evrope.

Priporočilo sheme XML digitalnega podpisa izvira iz W3C dokumenta *XML-Signature* (RFC3275). Dokument podrobneje opisuje izmenjavo dokumentov XML, določa sintakso in pravila procesiranja digitalnega podpisa, zagotavlja preverjanje podpisnika, integriteto podatkov in podporo nezanikanju, pri čemer upošteva lastnosti in prednosti interneta ter razširljivega opisnega jezika XML. Priporočilo lahko uporabimo za podpis dela ali vseh podatkov v XML, tekstovni in binarni obliki. Podpisani podatki so lahko vključeni v XML-Signature element preko sklica na URI, so del istega dokumenta kot XML-Signature element, so vsebovani v XML-Signature strukturi elementa ali pa je XML-Signature element del podatkovne strukture.

Za področje Evrope je ETSI pripravil priporočilo za *XML Advanced Electronic Signatures* (XAdES), ki priporočilu za XML-Signature dodaja elemente za varni digitalni podpis ter

elemente za dolgotrajno hranjenje digitalno podpisanih dokumentov. XAdES priporočilo temelji na *ETSI Electronic Signature Formats – TS 101 733 v1.3.1* priporočilu, ki podaja splošne pogoje za ustvarjanje varnega elektronskega podpisa in sledi priporočilu RFC 2630.

Priporočili določata tri oblike elektronskega podpisa:

- **Osnovni elektronski podpis**

  Ta oblika vključuje elektronski podpis in ostale osnovne informacije, priložene s strani podpisnika, za pravno veljavo pa vključuje še druge potrebne atribute podpisa, na primer referenco na politiko elektronskega podpisa, podpisane podatke, digitalni podpis in druge atribute. V osnovi ta oblika nudi identifikacijo podpisnika in zaščito celovitosti.

- **Elektronski podpis s časovnim žigom**

  Osnovna oblika elektronskega podpisa ne omogoča možnosti določitve časovnega okvirja (kdaj je bil elektronski podpis ustvarjen), zato ta oblika doda časovno oznako.

- **Elektronski podpis z vsemi podatki za overjanje**

  Tretja oblika elektronskega podpisa vsebuje referenco na vse podatke za možnost overjanja in njihove povzetke. Podatki za preverjanje veljavnosti elektronskega podpisa se lahko hranijo skupaj z osnovnim elektronskim podpisom ali ločeno.

Vse tri oblike se lahko dodajo priporočilu XAdES in mu dodajo elemente za zagotavljanje varnega elektronskega podpisa oziroma celotne informacije za preverjanje digitalnega podpisa v skladu z EU priporočili.

Predlagana shema za XML digitalni podpis je tako skladna z W3C in XAdES priporočili in vsebuje vse bistvene elemente digitalnega podpisa potrebne za ugotavljanje verodostojnosti podpisa, integritete podpisnih podatkov in identitete podpisnika.

E-SLOG za XML digitalni podpis priporoča nabor kriptografskih algoritmov na osnovi posebnega poročila ETSI (ETSI SR 002 176 V1.1.1 2003-03, Electronic Signatures and Infrastructures) in v Sloveniji ter svetu uveljavljene prakse.

Za končne uporabnike in overitelje priporoča ustvarjanje kriptografskih ključev dolžine 1024 bitov za obdobje uporabe do 5 let. Za overitelje, ki želijo svoje potrdilo uporabljati dlje, t.j. do 20 let, pa priporočajo dolžino ključa 2048 bitov.

Generiranje ključev in digitalno podpisovanje priporoča z uporabo algoritma RSA, kreiranje povzetkov pa z zgoščevalno funkcijo SHA-1.

Priporočila E-SLOG za elektronsko arhiviranje so sicer še v pripravi, a v njih vseeno najdemo nekaj napotkov, ki se jih moramo držati. Tako se kot standard za hranjenje vsebine priporoča uporaba dokumentov v obliki PDF ali XML. Kot temeljno sredstvo za zaščito zapisov je

prepoznan elektronski podpis. Elektronsko podpisan mora biti vsak objekt, ki je vstavljen v arhiv, ne glede na to, ali objekt vsebuje še druge varnostne atribute (podpise).

Kot kratkoročno arhiviranje se smatra hranjenje za obdobje neposredno po ustvarjenem elektronskem dokumentu. V arhiv vnesene elektronske dokumente je potrebno časovno žigosati. Časovni žig se lahko izvaja samo nad elektronskimi podpisi, v kolikor ti že sami vsebujejo povzetek dokumenta, ali nad celotnimi elektronskimi zapisi. Za ustvarjanje arhivskega gradiva se lahko uporablja lasten časovni žig (povzeto po [5,6]).

Poglavje 3 Predstavitev uporabljenih orodij

Za izdelavo zastavljenega računalniškega sistema smo uporabili več različnih komercialnih in prosto dostopnih programskih orodij. V naslednjem poglavju bomo na kratko predstavili, kje in zakaj se posamezna orodja uporabljajo, katere so njihove prednosti in glavne scenarije za lažjo predstavo njihove umestitve in uporabe v informacijskih sistemih.

3.1 IBM Transformation Extender

Velik izziv, s katerim se v današnjih časih sooča vse več organizacij, je integracija poslovnih in informacijskih sistemov. Informacijski sistemi so v večini sestavljeni iz več ločenih aplikacij, ki za svoje delovanje uporabljajo sporočila v različnih formatih. Veliko različnih formatov sporočil prinaša težave pri integraciji, in sicer predvsem s stroškovnega in časovnega vidika. Tekom razvoja posameznih aplikacij v informacijskem sistemu lahko prihaja do t.i. *informacijskih silosov.* To so ločeni sistemi (aplikacije), v katerih so informacije »ujete«, posledično pa jih je težko integrirati v ostale sisteme.

Drug velik izziv je spoštovanje in upoštevanje industrijskih standardov, ki se med drugim uveljavljajo ravno zato, da se organizacije izognejo informacijskim silosom. Za smotrno izmenjavo podatkov morajo organizacije poskrbeti, da so njihovi informacijski sistemi prilagojeni za izmenjavo podatkov po definiranih standardih, kot so EDI (Electronic Data Interchange), SWIFT (Society for Worldwide Interbank Financial Telecommunication), SEPA (Single Euro Payments Area), HL7 (Health Level Seven) in drugi. Sledenje definiranim standardom organizacijam omogoča lahko in standardno izmenjavo podatkov.

Programsko orodje IBM Transformation Extender je univerzalno, transakcijsko usmerjeno orodje za transformacijo in preverjanje pravilnosti podatkov. Orodje omogoča avtomatizacijo izmenjave podatkov med različnimi aplikacijami, od katerih vsaka uporablja svoj format sporočil in svoje podatkovne tipe. IBM Transformation Extender od izvornega sistema sprejme podatke v kakršnemkoli formatu in jih v pravilnem formatu preusmeri do ponornega sistema. Formati sporočil obsegajo vse od različnih aplikacijskih sporočil (tekstovne datoteke, datoteke MS Excel, sporočila XML, COBOL ...) do sporočil, namenjenih relacijskim

podatkovnim bazam (SQL), sporočilno usmerjenim vmesnim programom (JMS, MQ ...) in ostalim zunanjim sistemom. S tem spada orodje med tako imenovana orodja ESB (Enterprise Service Bus), ki se uporabljajo za preprostejšo izmenjavo sporočil med različnimi aplikacijami in informacijskimi sistemi (povzeto po [7]).

Orodje ponuja močan grafični uporabniški vmesnik, v katerem lahko sestavimo pretvorbo med različnimi formati podatkov, izvedemo preverjanje pravilnosti podatkov in pripravimo izvajalno okolje za transformacije sporočil brez uporabe programiranja. V trenutni verziji orodje podpira izvajalna okolja na več različnih strojnih platformah (IBM System P, IBM System Z, Intel x86, Sun SPARC, Intel Itanium ...) in operacijskih sistemih (Windows, Linux, AIX, z/OS, Solaris, HP).[8]

3.2 IBM DataPower Gateway

Ob uveljavitvi formata sporočil XML za izmenjavo podatkov preko spletnih storitev se je ponudila priložnost za izdelavo posebnih mrežnih naprav za zaščito, upravljanje in obravnavo sporočil XML. Prve takšne naprave so izdelali v podjetju DataPower in Vordel leta 1999, njihov cilj pa je bil pospešitev procesiranja sporočil XML s pomočjo namenske strojne opreme. V ta namen so razvili poseben čip, ki je sporočila XML obravnaval precej hitreje kot programske rešitve (t.i. »wire speed«).

V zadnjih letih so takšne naprave postale normalen način povezovanja informacijskih sistemov in aplikacij preko interneta in so uveljavljene v različnih integracijskih scenarijih. Večinoma se uporabljajo kot enotna vstopna točka podatkov v informacijske sisteme, za pospešitev in standardizacijo razvoja aplikativnih rešitev ter za integracijo različnih informacijskih sistemov.

Glavne prednosti uporabe so:

- Visoko zmogljivo procesiranje sporočil XML.
- Usmerjanje, filtriranje, nadzor pravilnosti in pretvorba podatkov.
- Izvajanje avtorizacije, avtentikacije in revizije na podatkovnih izmenjavah.
- Zaščita in upravljanje storitveno usmerjene arhitekture (SOA).
- Nadzor aplikativnih programskih vmesnikov (API-jev).

- Integracija aplikacij z zalednimi sistemi, oblačnimi storitvami in raznimi klienti [povzeto po [10]).

IBM DataPower Gateway je naslednja generacija družine namenskih fizičnih in virtualnih omrežnih naprav podjetja IBM (IBM DataPower SOA Appliances), namenjenih pospešitvi vzpostavitve spletnih storitev in XML komunikacije ter razširitvi SOA infrastrukture. DataPower Gateway je integracijska in varnostna platforma za mobilne, oblačne in aplikativne programske vmesnike (API-je), za vzpostavitev spletnih storitev in SOA infrastrukture ter integracijo med poslovnimi sistemi (B2B).

Naprava DataPower poenostavlja in optimizira upravljanje spletnih storitev in aplikacij ter izboljša zaščito storitev XML in IT. Z namensko strojno in programsko opremo naprava poveča zmogljivost in uporabnost IT sistemov, kar zmanjša operativne stroške in kompleksnost postavitve ter izboljša zmogljivosti delovanja.

Družina naprav DataPower v trenutni generaciji obsega naslednje modele:

1) Service Gateway appliance (XG45)

Model XG45 je nadgradnja modela XS40 in predstavlja vstopni model v svet naprav »SOA Gateway«. Njegova prednost je predvsem v hitri vpeljavi zaščite storitev, osnovanih na sporočilih XML, izvajanju dinamičnega usmerjanje glede na vsebino sporočila, predefinirani zaščiti pred napadi na XLM osnovane storitve (DOS – Denial of Service, SQL injection ...).

Glavne funkcionalnosti vstopnega modela so:

- Enkripcija/dekripcija sporočil XML s pomočjo namenskega strojnega modula za RSA operacije.
- Digitalno podpisovanje in preverjanje digitalnih podpisov.
- Izvajanje avtentikacije, avtorizacije in revizije nad sporočili XML.
- Predefinirana zaščita pred napadi preko sporočil XML.
- Dinamično usmerjanje in filtriranje sporočil XML.
- Pospeševanje procesiranja sporočil XML s pomočjo strojnega modula XG4.

- Nadzor in upravljanje kakovosti spletnih storitev.
- Povezovanje z več protokoli, kot so JMS, FTP, WebSphere MQ.
- Možnost dodatnega strojnega modula za procesiranje različnih formatov sporočil z dodano PKCS7 kriptografsko knjižnico.
- Možnost dodatnega strojnega varnostnega modula zagotavlja podporo standardu FIPS 140-2.
- Zadnja verzija programske opreme s certificiranim kriptografskim modulom prinaša podporo standardu FIPS 140-2 level 1.

2) Integration appliances (XI52, XI50B, XI50Z)

Model XI52 je paradni model družine DataPower. Omogoča vse, kar omogoča vstopni model, a zaradi boljših strojnih zmogljivosti ponuja boljše delovanje . Omogoča tudi integracijo s praktično vsemi protokoli za izmenjavo podatkov in ima možnost modula za izravnavanje obremenitev (t.i. »load balancing«), ki se poveže z družino IBM WebSphere Application Server in avtomatsko prepoznava obremenitve aplikativnih strežnikov ter temu primerno porazdeljuje zahtevke.

Ena izmed glavnih prednosti tega modela so t.i. binarne transformacije »kdorkoli s komerkoli«. S pomočjo zunanjih orodij (kot na primer IBM Transformation Extender) se oblikuje transformacijska predloga, to je navodilo za pretvorbo podatkov, IBM DataPower pa se uporabi kot izvajalno okolje, saj zaradi namenskih strojnih modulov omogoča izjemno hitro pretvorbo formatov sporočil.

3) B2B appliance (XB62)

S povečanjem potreb po izmenjavi podatkov med poslovnimi sistemi (B2B) je podjetje IBM pripravilo model XB62. V osnovi je model enak XG45 z dodano podporo B2B protokolom AS1, AS2, AS3 in ebMS. Model omogoča administracijo partnerjev preko standarda CPPA (ebXML Collaboration Protocol Profile Agreement), podporo sporočilom EDI, XML in binarnemu prometu, omogoča avtomatsko arhiviranje in brisanje B2B transakcij in visoko zmogljivost na račun namenske strojne podpore.

4) Edge appliance (XE82)

Še en model družine DataPower, ki je namenjan specifičnim potrebam organizacij. XE82 je zamišljen kot enotna točka za konfiguracijo in upravljanje. Naprava z namenskim kriptografskim modulom služi za vzpostavljanje in zaključevanje sej protokolov SSL in TLS, za pospešitev začetnih PKI rokovanj in predpomnjenjem sejnih ključev SSL in TLS za zmanjšanje potrebnih ponovitev rokovanj. Enako kot model XI52 ima možnost AO (Application Optimization) modula, s katerim lahko več naprav XE82 povežemo v samoizravnalno skupino (self-load balancing group) in s pomočjo zagotavljanja afinitete sej povečamo pretočnost in hkrati zagotavljamo enakomerno obremenitev sistema.

5) Caching appliance (XC10)

Model XC10 je namenjen predpomnjenju podatkov. V družino DataPower prinaša 240GB predpomnilnika, s katerim lahko izboljšamo elastičnost in skoraj linearno skaliranje aplikacij na učinkovit način.

6) IBM Workload Deployer

IBM Workload Deployer je evolucija IBM WebSPhere Cloudburst naprave. V osnovi si z družino DataPower deli samo strojno opremo. Namenjena je delu z vzorci in predlogami – to so predpripravljeni in konfigurirani virtualni strežniki z nameščeno vmesno programsko opremo. Za delovanje vzorcev in predlog je potreben ustrezen hipernadzornik, na katerega naprava namesti vzorce. Naprava ima možnost avtomatične elastičnosti, kar pomeni, da v primeru prekomerne obremenitve sama vzpostavi nove strežnike (iz vzorcev), da zadosti povečani potrebi pretočnosti. Po upadu obremenitve naprava tudi ustrezno zmanjša število delujočih strežnikov in tako poskrbi tudi za licenčne omejitve uporabe vmesne programske opreme.

7) Cast Iron appliance (XH40)

Cast Iron je podjetje v lasti IBM, ki je razvilo platformo za hitro in lahko integracijo s programsko opremo kot storitvijo (t.i. SaaS – Software as a Service) in z oblačnimi storitvami. Model XH40 si tako kot model Workload Deployer z družino DataPower deli samo strojno opremo.

Naprava je izvajalno okolje za integracije zasnovane v razvojnem okolju *WebSphere Cast Iron Studio*, ki, podobno kot orodje WTX, s pomočjo grafičnega vmesnika omogoča integracije aplikacij brez znanja programiranja.

Družina naprav DataPower pride v obliki strojne naprave za namestitev v strežniške omare ali kot rezina za namestitev v strežniške šasije IBM BladeCenter. IBM ponuja modele družine DataPower tudi kot navidezne naprave v obliki VMWare ESX virtualnih slik za namestitev na hipernadzornik (povzeto po [9]).

3.3 OpenSSL

OpenSSL je programska knjižnica, namenjena zaščiti komunikacijskih poti med različnimi aplikacijami in informacijskimi sistemi.

Programska knjižnica je odprtokodni projekt, v katerem želi mednarodna skupnost prostovoljno priskrbeti robustno, kvalitetno in zmogljivo ogrodje za delo z varnostnimi protokoli TLS (Transport Layer Security) in SSL (Secure Socket Layer). Ogrodje vključuje tudi splošno namensko kriptografsko knjižnico.

Orodje OpenSSL je licencirano v okviru licence Apache, kar pomeni, da je orodje prosto za uporabo in se ga lahko uporablja tudi v komercialne namene z upoštevanjem preprostih licenčnih omejitev.

Verzije programski knjižnice so na voljo za praktično vse na sistemu UNIX osnovane operacijske sisteme (vključujoč Solaris, Linux, Mac OS X), OpenVMS in Microsoft Windows okolja. IBM je priskrbel tudi podporo za svoj operacijski sistem System i (OS/400) (povzeto po [11]).

Različica OpenSSL orodja za operacijski sistem Windows se imenuje OpenSSL for Windows oziroma GnuWin32 [12].

3.4 cURL

Programsko orodje za ukazno vrstico in programska knjižnica cURL je namenjena prenosu podatkov v obliki sintakse URL. Podpira veliko različnih protokolov za prenos podatkov (FTP, FTPS, SCP, Telnet, SMTP, HTTP ...) in deluje na praktično vseh platformah (Windows, Unix, Linux, OS/2, Android, QNX, DOS ...). Dandanes se orodje večinoma uporablja v ukaznih vrsticah in programskih skriptah, v avtomobilih, televizijah, usmerjevalnikih, tiskalnikih, mobilnih telefonih in še v mnogih napravah, ki se povezujejo v internet.

Programsko orodje je prosto dostopno in na voljo kot »open source/free software« (v okviru MIT/X licenc), kar pomeni, da se knjižnico in samo orodje lahko prosto uporablja in spreminja v kakršnekoli namene (povzeto po [13]).

3.5 SoapUI

Odprtokodna in prosto dostopna platforma SoapUI podjetja SmartBear je splošno uporabno orodje za avtomatizacijo funkcionalnega, regresijskega in obremenitvenega testiranja.

Vsebuje enostaven grafični vmesnik, v katerem lahko hitro pripravimo teste spletnih in REST storitev, za katere orodje iz dokumenta WSDL kreira testne zahtevke in naslove. Lahko si pripravimo tudi t.i. »mock« storitve ali testne primere.

Orodje vsebuje nabor orodij za ukazno vrstico, s katerimi lahko funkcionalne in obremenitvene teste poganjamo iz praktično kateregakoli časovnika.

Plačljiva verzija orodja poleg vsega zgoraj naštetega vsebuje še orodja za izdelavo poročil, celo vrsto funkcij za prihranek časa in povečanje produktivnosti ter podporo preko forumov in elektronske pošte (povzeto po [14]).

3.6 SMS Gateway

V splošnem je programska oprema SMS Gateway namenjena sprejemanju in pošiljanju sporočil sistema kratkih sporočil (SMS) preko telekomunikacijskih omrežij. Med drugim običajno omogoča tudi pretvorbo različnih sporočil v format sporočil SMS, kot na primer pretvorbo elektronske pošte v sporočilo SMS.

Običajno je SMS Gateway del obširnejše programske rešitve »SMS Center (SMS-SC Short Message Service – Service Center)«. SMS-SC je pravzaprav mrežni element v mobilnem telefonskem omrežju, katerega namen je shranjevanje, posredovanje, pretvarjanje in pošiljanje sporočil SMS.

SMS Gateway pa je lahko tudi samostojna programska rešitev, ki uporabniku omogoča, da si na mobilni napravi ustvari lasten sistem pošiljanja sporočil SMS.

Prosto dostopna SMS Gateway aplikacija, ki jo je razvil Karel Kyovsky (nadimek b00lean) za operacijski sistem Android, je na voljo v Google Play Store [15]. Mobilna aplikacija omogoča:

- pošiljanje sporočil SMS;
- periodično preverjanje elektronske pošte preko POP3 protokola in pretvorbo elektronske pošte v format sporočila SMS;
- prepošiljanje prejetih sporočil SMS v formatu elektronske pošte preko protokola SMTP;
- posredovanje sporočil SMS preko protokola HTTP GET.

Poglavje 4 Opis razvitega sistema

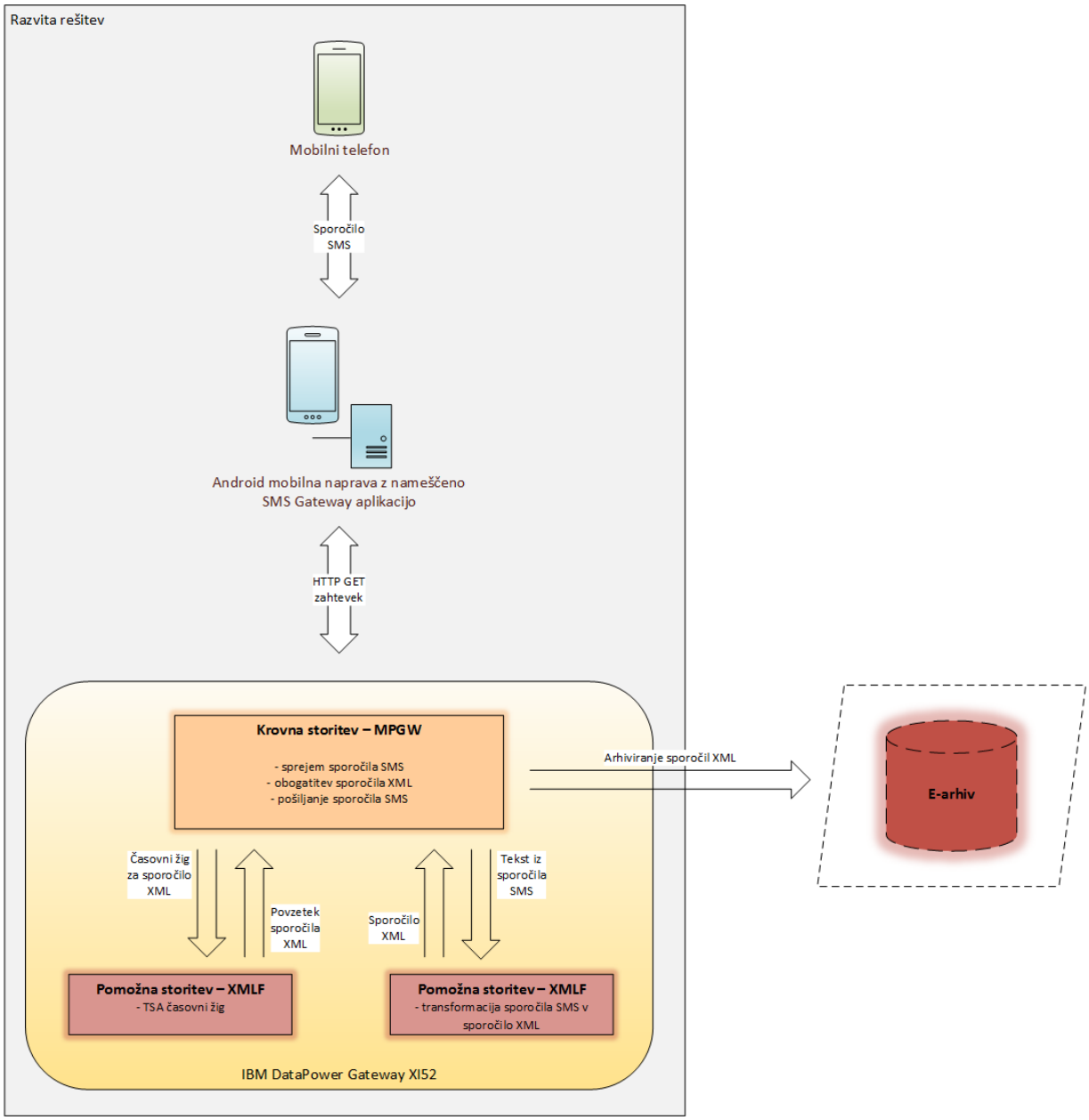
Računalniški sistem za transformacijo sporočil SMS v digitalno podpisana in časovno overovljena sporočila XML smo izdelali s pomočjo orodij, opisanih v prejšnjem poglavju. Vsako orodje je bilo uporabljeno za pripravo manjšega sklopa v celotni rešitvi in/ali za testiranje posameznega dela in celotne rešitve.

Držali smo se priporočil in standardov, ugotovljenih v drugem poglavju, kjer pa to iz objektivnih razlogov ni bilo možno (na primer kvalificirano digitalno potrdilo), smo za izdelavo rešitve uporabili tehnično enakovredne prijeme, ki pa v poslovanju niso dovoljeni (na primer samo-podpisana digitalna potrdila).

4.1 Arhitektura

Uporabnik testnega sistema preko mobilnega telefona pošlje sporočilo SMS z definirano vsebino na mobilno napravo z nameščeno SMS Gateway aplikacijo. Aplikacija preko protokola HTTP GET prejeto sporočilo SMS posreduje na krovno spletno storitev na napravi DataPower. Naprava DataPower iz prejetega obvestila izlušči vsebino tekstovnega sporočila in metapodatke ter jih preusmeri na pomožno spletno storitev na napravi DataPower. Storitev vsebino sporočila SMS pretvori v sporočilo XML in ga vrne krovni spletni storitvi na napravi DataPower. Nad transformiranim sporočilom XML se izvede kreiranje izvlečka sporočila. Povzetek se pošlje drugi pomožni storitvi, ki v sistemu predstavlja TSA. Storitev prejetemu povzetku sporočila doda časovni žig in ga vrne krovni storitvi. Krovna storitev sporočilu XML doda metapodatke, časovni žig in ovojnico SOAP. Celotno sporočilo XML, vključno z ovojnico SOAP, digitalno podpiše in ga vrne kot odgovor. Ob uspešni izvedbi transformacije sporočila SMS naprava DataPower uporabniku pošlje sporočilo SMS.

Sistem ima zasnovano večnivojsko osnovno obravnavo napak, in sicer se v primeru napake izvajanje sistema ustavi, uporabnik pa dobi obvestilo o napaki. Napake se lovijo na vseh nivojih sistema.



Slika 4-1: Visokonivojska arhitektura razvite rešitve

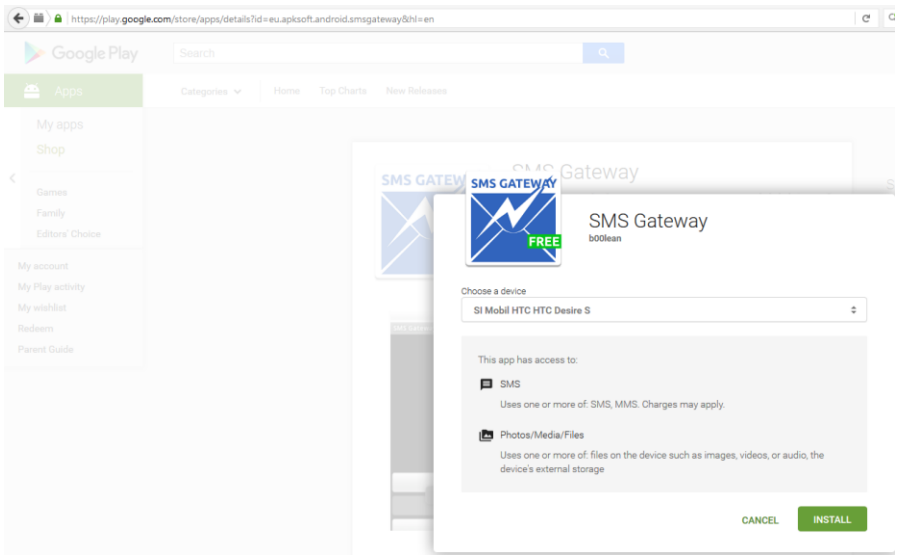
4.2 SMS Gateway aplikacija

Prvi korak k izdelavi rešitve je bila premostitev tehnične prepreke pri pošiljanju sporočil SMS na navidezno napravo DataPower. V ta namen smo raziskali nekaj različnih aplikacij SMS Gateway za mobilne naprave z operacijskim sistemom Android, ki so prosto dostopne na

Googlovi spletni trgovini Play Store, in se nazadnje odločili za uporabo SMS Gateway aplikacije razvijalca z vzdevkom b00lean.

4.2.1 Namestitev in nastavitev aplikacije

Aplikacijo SMS Gateway smo poiskali preko iskalnika v Google Play Store in jo namestili s pomočjo čarovnika za nameščanje mobilnih aplikacij.

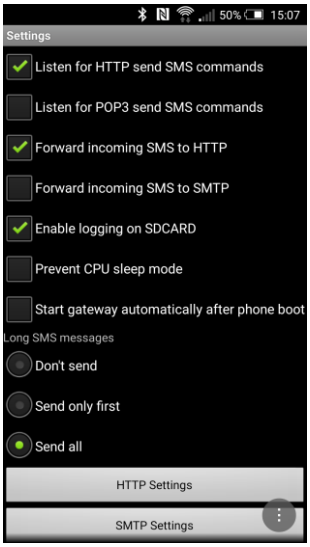


Slika 4-2: Namestitev SMS Gateway aplikacije preko Google Play Store

Ob zagonu aplikacije se pojavi možnost različnih nastavitev. Za posredovanje sporočil SMS je bilo potrebno v meniju *»Settings«* obkljukati možnosti:

- *»Listen for HTTP send SMS commands«* (omogoči pošiljanje sporočil iz naprave DataPower na mobilne naprave)
- *»Forward incoming SMS to HTTP«* (prepošlje sporočilo SMS na napravo DataPower)

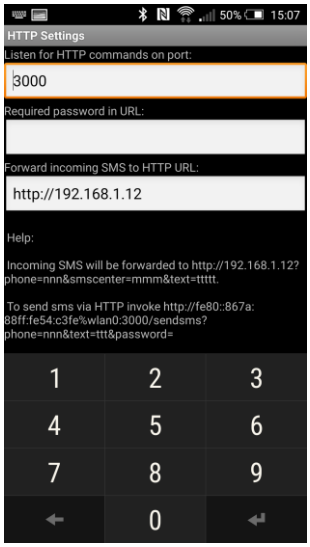
Možnost »*Enable logging on SDCARD*« smo uporabili za beleženje dogajanja v dnevnik in odpravljanje napak ob testiranju sistema.



Slika 4-3: Primer uporabljenih možnosti aplikacije SMS Gateway

Da je aplikacija SMS Gateway lahko prejemala sporočila na mobilnem telefonu, smo morali vnesti številko vrat, višjo od 1024, saj so številke vrat do vključno 1024 v sistemih Unix (izpeljanka katerega je tudi operacijski sistem Android) rezervirane za administrativnega uporabnika (root). V podmeniju »*HTTP Settings*« smo v vnosnem polju »*Listen for HTTP commands on port*« nastavili številko vrat 3000. Naprava DataPower tako pošilja zahtevke na IP naslov mobilne naprave in vrata številka 3000.

Nadalje smo v istem podmeniju v vnosnem polju »*Forward incoming SMS to HTTP URL*« nastavili naslov URL spletne storitve na napravi DataPower. V pomoč nam aplikacija ponudi, v kakšni obliki je potrebno pripraviti klic za pošiljanje sporočila SMS in na kateri naslov bo aplikacija prejeto sporočilo SMS posredovala.



Slika 4-4: Primer nastavitev za prepošiljanje in pošiljanje sporočil SMS

Ustrezno nastavljeno aplikacijo smo morali zagnati (Status: running) in od tega trenutka dalje so se vsa prejeta sporočila SMS prepošiljala na napravo DataPower.

Slika 4-5: Zagon aplikacije z nastavljenimi možnostmi

4.2.2 Opis sporočila SMS in metapodatkov

Sistem kratkih sporočil SMS je dvosmerna storitev pošiljanja kratkih tekstovnih sporočil preko telefonskih, spletnih in mobilnih komunikacijskih sistemov. Za delovanje uporablja standardizirane komunikacijske protokole (GSM) in omogoča izmenjavo sporočil SMS med stacionarnimi in mobilnimi telefonskimi napravami.

Sporočilo SMS je specificirano s standardom ETSI GSM03.40 in 03.38. Vsebuje lahko do 160 znakov, kjer je vsak znak predstavljen v skladu s 7-bitno privzeto abecedo GSM. Poleg vsebine sporočilo SMS vsebuje tudi metapodatke, kot na primer informacije o telefonski številki pošiljatelja, telefonsko številko SMS-SC in podatke o uporabljenem prenosnem protokolu, časovni žig [16].

V testnem sistemu smo se osredotočili na vsebino sporočila SMS. Vsebina je definirana z vnaprej določenimi pomenskimi polji, ločenimi z vejico. Sporočilo se zaključi s podpičjem. Definirana polja so zamišljena na podlagi osebnih izkušenj z operaterji in poznavanja delovanja telekomunikacijskih informacijskih sistemov.

Sestava vsebine sporočila SMS je naslednja:

< ime_naročnika > , < priimek_naročnika > , < rojstni_datum > , < šifra_naročnika > , <koda_storitve > , < datum_željene_aktivacije > ;

Pomen posameznih polj:

Polje	**Pomen**
ime_naročnika	Ime naročnika
priimek_naročnika	Priimek naročnika
rojstni_datum	Rojstni datum naročnika
šifra_naročnika	Šifra naročnika pri operaterju
koda_storitve	Koda storitve
datum_željene_aktivacije	Datum aktivacije izbrane storitve

Tabela 4-1 Pomen posameznih polj sporočila SMS

Pomenska polja so različnih podatkovnih tipov:

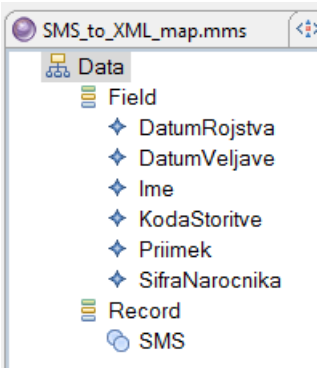
Pomensko polje	**Podatkovni tip**
ime_naročnika	String
priimek_naročnika	String
rojstni_datum	Date
šifra_naročnika	Number
koda_storitve	String
datum_željene_aktivacije	Date

Tabela 4-2 Podatkovni tipi pomenskih polj sporočila SMS

4.3 Transformacija WTX

Programsko orodje WTX smo uporabili za pretvorbo sporočila SMS v sporočilo XML. V razvojnem okolju IBM WTX Design Studio, osnovanem na platformi Eclipse, smo razvili transformacijsko predlogo, ki izvajalnemu okolju (v našem primeru napravi DataPower) poda navodila za pretvorbo sporočil.

Razvoj transformacijske predloge se prične z definiranjem strukture sporočil. S pomočjo čarovnika WTX za uvoz tekstovnih datotek smo definirali format sporočila SMS – podatkovne tipe, ločilo med posameznimi polji in znak za zaključek besedila. Orodje WTX si strukturo sporočila shrani v objekt Type Tree. Objekt sestavlja zapis celotnega sporočila »Data«, opis posameznega polja znotraj kategorije »Field« in opis celotnega sporočila v kategoriji »Record«.



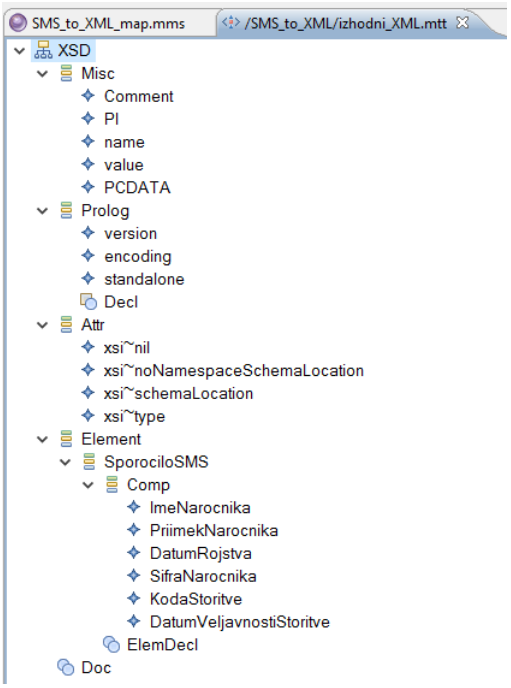
Slika 4-6: WTX Type Tree objekt za sporočilo SMS

Definicijo sporočila XML smo podali z ročno pripravljeno shemo sporočila XML v obliki:

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="SporociloSMS">
    <xs:complexType>
      <xs:sequence>
        <xs:element type="xs:string" name="ImeNarocnika"/>
        <xs:element type="xs:string" name="PriimekNarocnika"/>
        <xs:element type="xs:date" name="DatumRojstva"/>
        <xs:element type="xs:integer" name="SifraNarocnika"/>
        <xs:element type="xs:string" name="KodaStoritve"/>
        <xs:element type="xs:date" name="DatumVeljavnostiStoritve"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

Slika 4-7: Shema sporočila XML

Čarovnik WTX za uvoz sheme XML nam je sestavil nov objekt Type Tree z opisom strukture sporočila XML:



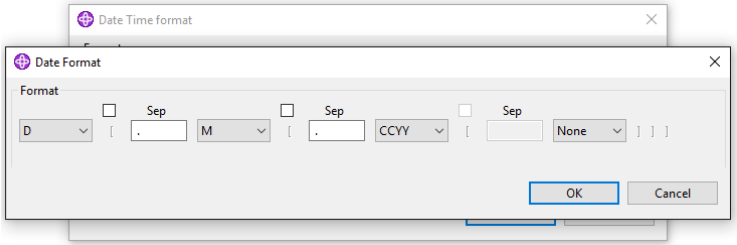
Slika 4-8: WTX Type Tree objekt za sporočilo XML

WTX transformacijska predloga za delovanje potrebuje vhodne in izhodne kartice. Vsako kartico je potrebno poimenovati, ji dodeliti ustrezni objekt Type Tree in povedati, katero podatkovno strukturo iz objekta Type Tree lahko kartica kot vhod pričakuje. Podati je potrebno tudi datoteko, ki vsebuje testne podatke in s katero bomo testirali pravilnost izvajanja transformacijske predloge.

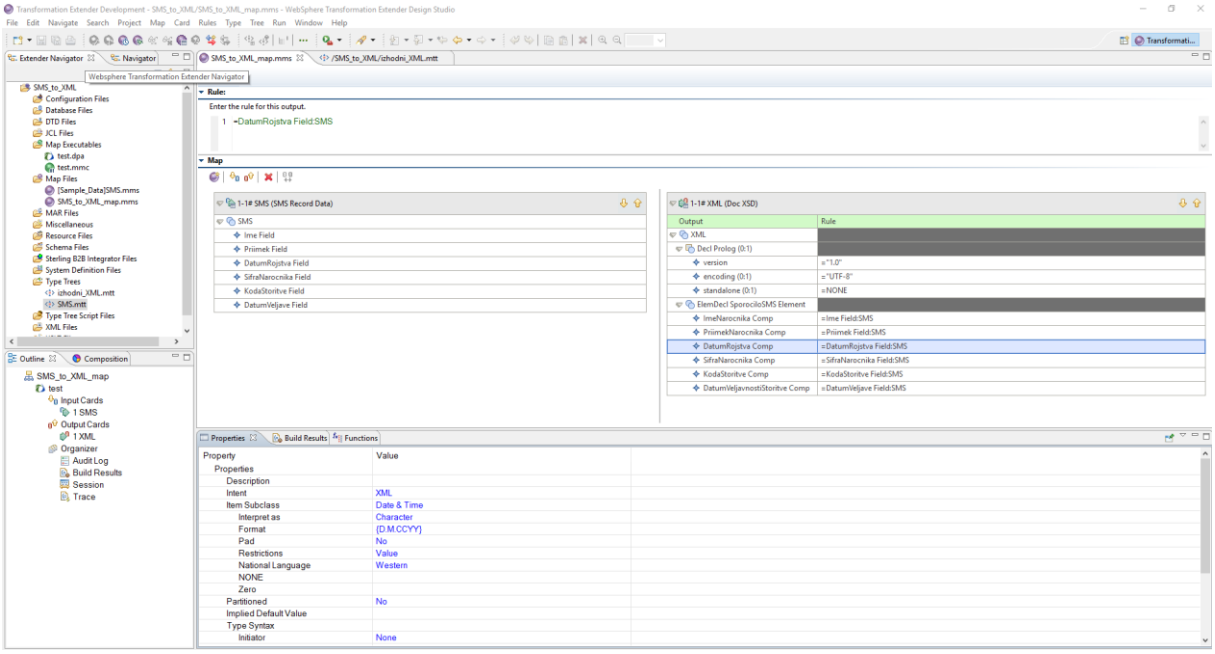
Vhodna kartica je v našem primeru struktura sporočila SMS, izhodna kartica pa struktura sporočila XML.

Podatke iz enega sporočila preslikamo v željen podatek v drugem sporočilu. Na podatkih lahko vršimo dodatne funkcije, kot npr. pretvorbe datumov, ki so nam v pomoč pri preverjanju pravilnosti vhodnih in zagotavljanju pravilnosti izhodnih podatkov.

V transformaciji smo uporabili preverjanje pravilnosti vnešenih datumov.

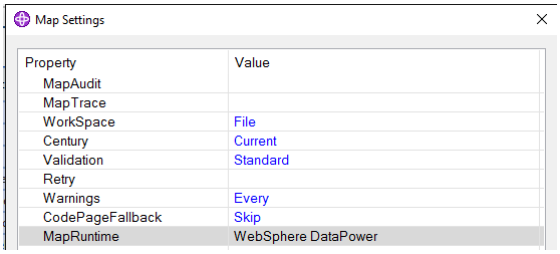


Slika 4-9: Format datuma v transformaciji WTX za sporočilo XML



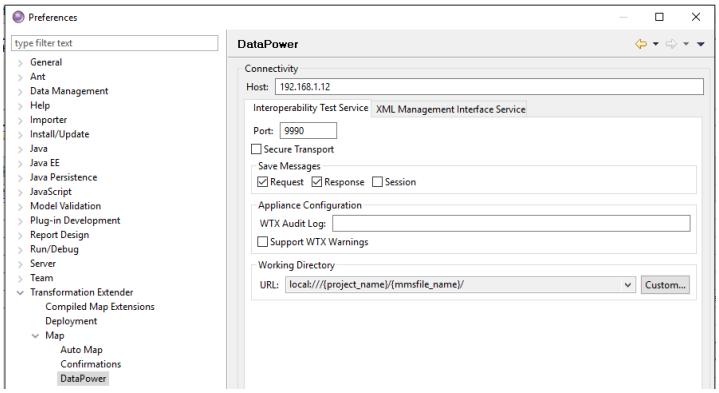
Slika 4-10: Izdelava WTX transformacijske predloge za pretvorbo sporočila SMS v sporočilo XML

Delovanje transformacijske predloge WTX lahko preverimo na lokalnem izvajalnem okolju znotraj programskega orodja WTX ali pa orodje WTX povežemo z zunanjo napravo DataPower. V nastavitvah izvajalnega okolja transformacijske predloge izberemo napravo DataPower.



Slika 4-11: Nastavitev izvajalnega okolja WTX transformacijske predloge

Za povezavo z napravo DataPower moramo v orodju WTX nastaviti podatke za povezavo z DataPower Interoperability Test Service, ki omogoča klic in izvajanje transformacijske predloge na napravi DataPower, in povezavo z DataPower XML Management Interface Service, ki omogoča prenos transformacijske predloge na napravo DataPower. Oboje se nastavi v meniju »Preferences«



Slika 4-12: Primer nastavitev WTX zunanjega izvajalnega okolja na DataPower

Transformacijsko predlogo poženemo z ukazom Run. Orodje WTX preko klica DataPower Interoperability Test Service na napravo DataPower pošlje testni datoteki, nastavljeni v transformacijski predlogi, in požene transformacijsko predlogo. Rezultate transformacije lahko preverimo v orodju WTX Design Studio.

4.4 Priprava samo-podpisanega digitalnega potrdila

Digitalno podpisovanje sporočil XML se je uveljavilo kot eden najzanesljivejših načinov, kako zagotoviti pristnost elektronskih sporočil. Po ZEPEP je šele varen digitalni podpis, overjen s kvalificiranim zaupanja vrednim digitalnim potrdilom, enakovreden lastnoročnemu podpisu. Za potrebe izdelave testnega sistema smo uporabili zasebni ključ in samopodpisano digitalno potrdilo.

Zasebni ključ in digitalno potrdilo smo pripravili z verzijo orodja OpenSSL za operacijski sistem Windows. Po namestitvi programa smo kot administrator sistema zagnali ukazno vrstico programa OpenSSL in vnesli ukaz za kreiranje 1024-bitnega zasebnega ključa z uporabo algoritma RSA.

```
OpenSSL> genrsa -out RSA_kljuc.pem 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.........++++++
.....++++++
e is 65537 (0x10001)
OpenSSL>
```

Slika 4-13: Primer generiranja zasebnega ključa

V naslednjem koraku smo morali pripraviti CSR zahtevek, v katerem smo navedli nekaj osnovnih podatkov, za koga se samopodpisano digitalno potrdilo izdaja (država, mesto, organizacija, oddelek, elektronski naslov ...).

```
OpenSSL> req -new -key RSA_kljuc.pem -out CSR.pem -config "C:\Program Files (x86
)\GnuWin32\share\openssl.cnf"
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:SI
State or Province Name (full name) [Some-State]:Ljubljana
Locality Name (eg, city) []:Ljubljana
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Testna organizacija
Organizational Unit Name (eg, section) []:Testni oddelek
Common Name (eg, YOUR name) []:Tomaz
Email Address []:Tomaz@test.si

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Slika 4-14: Primer generiranja CSR zahtevka

V zadnjem koraku smo z uporabo CSR zahtevka in zasebnega ključa generirali še samopodpisano digitalno potrdilo s časom veljavnosti eno leto.

```
OpenSSL> req -x509 -days 365 -key RSA_kljuc.pem -in CSR.pem -out Digitalno_potrd
ilo.pem -config "C:\Program Files (x86)\GnuWin32\share\openssl.cnf"
Loading 'screen' into random state - done
OpenSSL>
```

Slika 4-15: Primer generiranja digitalnega potrdila

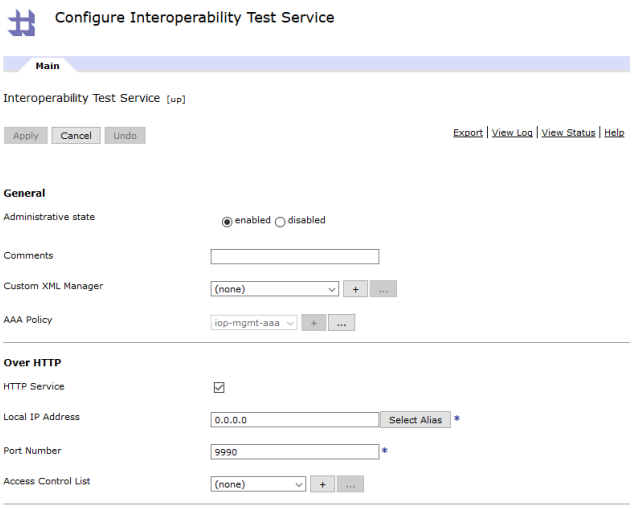
4.5 DataPower konfiguracija

Glavnina testnega sistema je zasnovana okoli navidezne naprave DataPower XI52. Napravo DataPower lahko razdelimo v več aplikativnih, logično ločenih domen, ki jih lahko povsem ločimo tudi na nivoju mrežnih nastavitev. Tako lahko eno domeno uporabimo v demilitariziranem območju, drugo pa v intranetu. Osnovne administrativne in omrežne nastavitve se opravljajo v osnovni domeni, zato smo zaradi poenostavljanja izvedbe testnega sistema tudi vse storitve pripravili v tej domeni.

4.5.1 Priprava izvajalnega okolja

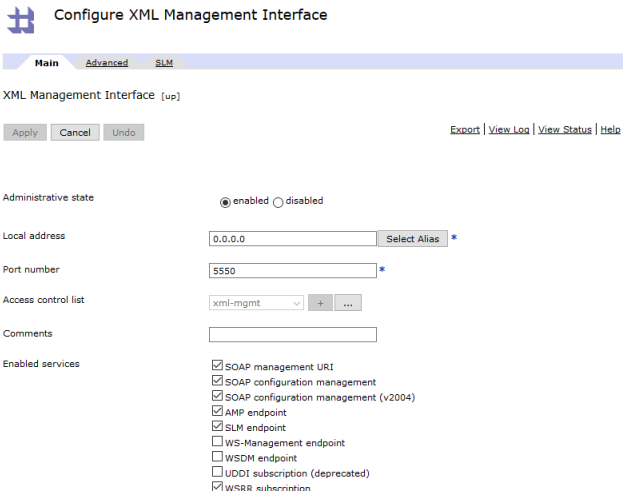
V poglavju 4.3 smo ugotovili, da orodje WTX za uporabo izvajalnega okolja na napravi DataPower potrebuje povezavo z DataPower Interoperability Test Service, katero je potrebno

na napravi najprej pognati. Za testni sistem smo storitev vklopili za delovanje preko protokola HTTP.



Slika 4-16: DataPower Interoperability Test Service storitev

Da smo iz orodja WTX lahko nameščali transformacijske predloge in poganjali teste, smo morali na napravi DataPower vklopiti tudi enega izmed treh administrativnih vmesnikov – XML Management Service.



Slika 4-17: DataPower XML Management Service administrativni vmesnik

4.5.2 Obogatitev sporočila XML

Družina naprav DataPower nam omogoča širok nabor obdelav sporočil XML. Osnovne akcije obdelave sporočil XML, ki so na voljo, tako ponujajo možnosti filtriranja sporočil glede na vsebino in naslov IP, digitalno podpisovanje in preverjanje digitalnega podpisa, preverjanje

pravilnosti zahtevka glede na definirane sheme (na primer preverjanje strukture zapisa XML), transformacije XSLT, usmerjanje zahtevkov glede na vsebino ali druge parametre, avtentikacijo, avtorizacijo in revizijo ter še kar nekaj dodatnih akcij, ki se skrivajo v akciji »Advanced«.

Slika 4-18: Osnovne akcije za manipulacijo sporočil XML na napravi DataPower

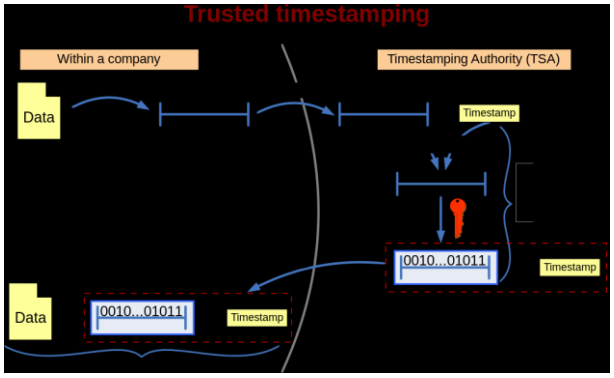
Z uporabo akcije »Transform« lahko izvajamo t.i. binarne preslikave »kdorkoli s komerkoli« ali pa preprosto uporabimo programski jezik XSL za manipulacijo sporočila XML. V tej akciji smo na primer nastavili, da se izvede WTX transformacijska predloga, ki nam je omogočila pretvorbo sporočila SMS v sporočilo XML.

Sporočilo XML pa smo nadalje morali opremiti še z metapodatki in časovnim žigom ter ga na koncu digitalno podpisati.

4.5.2.1 Časovni žig

V splošnem je časovni žig digitalni zapis, ki zagotavlja podpis elektronskega dokumenta v določenem časovnem trenutku in sicer na način, da povezuje datum in čas podpisa ter podatke v elektronski obliki. Časovni žig dokazuje obstoj elektronskega dokumenta pred časom, navedenim v časovnem žigu, poleg tega pa omogoča preverbo, da se od časa žigosanja elektronski dokument ni spremenil.

Storitev varnega časovnega žiga, ki jo ponujajo TSA, pri elektronskih dokumentih nastopa kot zunanja, verodostojna entiteta, ki ji pošljemo z zgoščevalno funkcijo narejen izvleček elektronskega dokumenta. Strežnik časovnega žigosanja izvlečku dokumenta doda čas prejema povzetka, naredi nov izvleček kombinacije izvlečka dokumenta in časa prejema dokumenta, novemu izvlečku doda čas obdelave in vse skupaj podpiše s svojim zasebnim ključem – to je časovni žig. Dokument lahko preverimo tako, da z isto zgoščevalno funkcijo naredimo nov izvleček dokumenta in ga primerjamo s tistim v časovnem žigu (povzeto po [17]).



Slika 4-19: Shema delovanja varnega časovnega žiga [21]

Za izdelavo testnega sistema smo pripravili posebno storitev, ki simulira zunanjo storitev TSA. Storitev na povzetku sporočila XML s pomočjo transformacije XSLT izvede proceduro dodajanja časovnega žiga. V akciji »Transform« smo s transformacijo XSLT in uporabo razširjenih funkcij DataPower XSLT koprocesorja in dodatnih časovnih funkcij XSL jezika:

- xmlns:dp="http://www.datapower.com/extensions"
- xmlns:date="http://exslt.org/dates-and-times"

izračunali in sestavili pravi format trenutnega časa.

S pomočjo funkcije time-value() smo dobili pretečeni čas (naprava DataPower interni čas beleži v milisekundah od 1.1.1970 naprej), ga prišteli datumu in uredili za izpis v željenem formatu.

```
<xsl:variable name="cas_v_ms" select="dp:time-value()"/>
<xsl:variable name="cas_v_s" select="$cas_v_ms div 1000"/>
<xsl:variable name="cas" select="date:duration($cas_v_s)"/>
<xsl:variable name="cas_dolgi_format" select="date:add('1970-01-01T00:00:00Z',$cas)"/>
<xsl:variable name="casEST" select="date:add($cas_dolgi_format,'PT3600S')"/>
<xsl:variable name="trenutni_cas" select="substring($casEST,1,23)"/>
```

Slika 4-20: Izračun trenutnega časa na napravi DataPower

Čas prejema povzetka dokumenta smo v isti transformaciji XSLT dodali k sporočilu XML.

```
<CasovniZig>
    <CasPrejemaZahtevka>
        <xsl:value-of select="$trenutni_cas"></xsl:value-of>
    </CasPrejemaZahtevka>
</CasovniZig>
```

Slika 4-21: Obogatitev sporočila XML s časom prejema

Povzetek dokumenta smo pridobili z uporabo DataPower zgoščevalne funkcije. Funkcija kot parameter sprejme dokument XML in algoritem, s katerim bo kreirala povzetek dokumenta. Privzeta nastavitev je povzetek s pomočjo SHA1 zgoščevalne funkcije.

```
<Povzetek>
    <xsl:value-of select="dp:c14n-hash($DokumentInZig, false())"/>
</Povzetek>
```

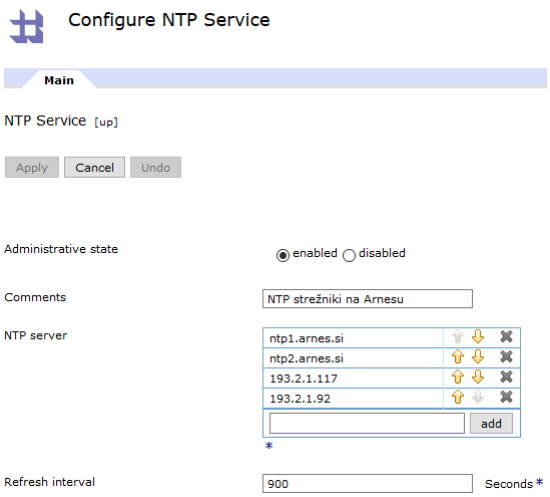
Slika 4-22: Uporaba DataPower zgoščevalne funkcije

TSA storitev mora biti zaupanja vredna, kar doseže z verodostojnim digitalnim potrdilom in politiko upravljanja, ter časovno usklajena s časovnimi strežniki. V ta namen se uporablja eden izmed najstarejših internetnih protokolov – NTP.

NTP je internetni mrežni protokol, namenjen časovni sinhronizaciji med računalniškimi sistemi. Protokol uporablja hierarhično mrežo časovnih strežnikov. Vsak nivo hierarhije se imenuje Stratum in ima dodeljeno številko nivoja hierarhije. Stratum 0 časovni strežniki so izjemno natančne časovne naprave kot npr. atomske (cezijeve, rubidijeve) ali GPS ure. Takšni časovni strežniki so znani tudi kot referenčne ure.

V Sloveniji je en izmed ponudnikov NTP časovnih strežnikov Zavod Arnes. Njihova storitev obsega dva časovna strežnika za točen čas nivoja Stratum 1, ki svojo notranjo uro usklajujeta na GPS uro in druge NTP Stratum 1 strežnike[18].

Naprava DataPower omogoča povezavo s strežniki NTP, preko katerih lahko sinhronizira svojo interno uro. Za izdelavo testnega sistema smo storitev DataPower NTP povezali z Arnesovimi časovnimi strežniki in s tem zagotovili časovno sinhronizacijo naprave.



Slika 4-23: DataPower NTP storitev

4.5.2.2 Digitalni podpis

Elektronski podpis je kakršnakoli oznaka, narejena z elektronskimi mediji z namenom, da označi nek dokument ali datoteko. Digitalni podpis je izpeljanka elektronskega podpisa, pri kateri za označbo dokumenta uporabljamo kriptografske prijeme.

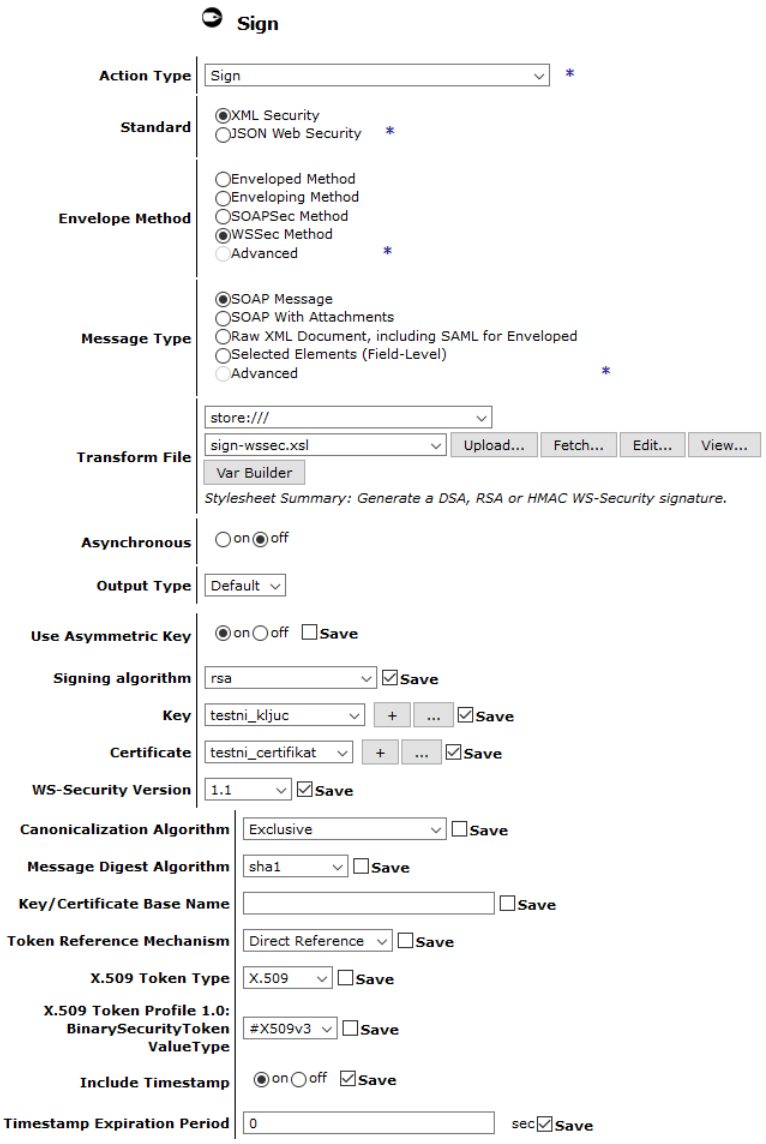
Danes se dokumente večinoma digitalno podpisuje z uporabo asimetrične kriptografije (ki zahteva obstoj infrastrukture javih ključev – angl. PKI, public key infrastructure). Uporabnik dokument zašifrira s svojim zasebnim ključem, odšifrira pa ga lahko vsak, ki pozna njegov javni ključ – to se šteje kot preverjanje digitalnega podpisa. Uporaba asimetrične kriptografije na veliko dokumentih je počasna, zato se v praksi uporablja digitalno podpisovanje povzetka dokumenta. Povzetek je običajno niz znakov dolžine 160 bitov (pridobljenih z uporabo enosmernih zgoščevalnih funkcij), ki enolično določa vsebino dokumenta. Takšen povzetek se potem podpiše z zasebnim ključem.

Dandanes se v digitalnih podpisih najpogosteje uporablja zgoščevalna funkcija SHA-1 z RSA ključi dolžine 1024-bitov (povzeto po [19]).

Zasebne ključe in samopodpisana digitalna potrdila smo izdelali z orodjem OpenSSL.

Ena izmed glavnih funkcionalnosti naprave DataPower za zaščito sporočil XML je uporaba kriptografskih prijemov. Akcija »Sign« v politiki obdelave zahtevkov omogoča digitalno podpisovanje z uporabo različnih algoritmov in digitalnih potrdil. Ponuja širok nabor možnosti nastavitev podpisovanja na nivoju sporočila XML, ovojnice SOAP ali na posameznih elementih sporočila, različne metode podpisovanja, različne šifrirne algoritme in še precej drugih nastavitev.

To akcijo smo uporabili v pomožni storitvi časovnega žigosanja (poglavje 4.5.3.2) in v krovni storitvi (poglavje 4.5.3.3).



Slika 4-24: Primer nastavitev akcije Sign na napravi DataPower

4.5.3 Izpostavitev spletnih storitev

Naprava DataPower omogoča pripravo več različnih storitev, namenjenih specifičnim področjem uporabe. Osnovne storitve so:

1) **XML Firewall (XMLF)**

   Storitev je namenjena procesiranju in zaščiti sporočil XML.

2) **Web Service Proxy (WSP)**

Storitev je namenjena virtualizaciji in procesiranju spletnih storitev, podanih z opisom v datoteki WSDL.

3) **Multi-Protocol Gateway (MPGW)**

Storitev je namenjena integracijskim scenarijem, ki zahtevajo spremembe protokolov in formatov sporočil.

4) **Web Application Firewall (WAF)**

Storitev je namenjena zaščiti spletnih aplikacij.

Slika 4-25: DataPower osnovne storitve

Način nastavljanja posamezne storitve sledi enakemu principu. Vsaka storitev potrebuje:

1) Poslušalca – objekt, ki posluša na definiranem protokolu, naslovu in vratih.

2) Naslov zalednega sistema – to je lahko vezana storitev na napravi DataPower, zunanji sistem ali t.i. »loopback« oziroma povratna zanka, kjer klic ne zapusti naprave.

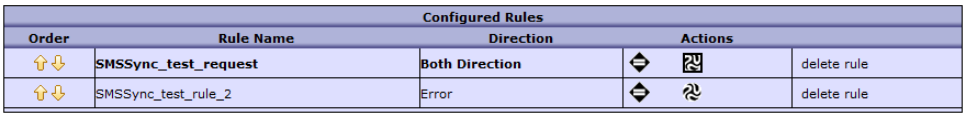
3) Politiko obdelave zahtevkov – za vsako vrsto zahtevka določimo pravila, po katerih bo zahtevek procesiran.

4.5.3.1 Storitev za binarno transformacijo sporočil SMS v sporočila XML

Storitev smo pripravili z uporabo storitve XMLF. Poslušalca smo nastavili, da posluša na vseh vhodnih vmesnikih (IP naslov 0.0.0.0) in vratih 3000. Vsak zahtevek, ki na napravo DataPower vstopi na vratih 3000, se procesira v tej storitvi.

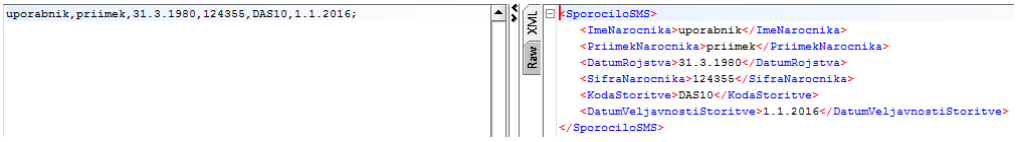
Vhodni zahtevek je v obliki tekstovne datoteke, zato smo morali storitev XMLF nastaviti, da procesira ne-XML promet.

V politiki obdelave zahtevkov smo definirali dve pravili: prvo pravilo v smeri odjemalec – strežnik - odjemalec in drugo, ki se sproži v primeru napak ob procesiranju zahtevkov.



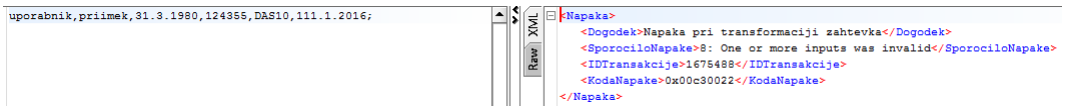
Slika 4-26: Politika obdelave zahtevkov za binarno transformacijo

Prvo pravilo sprejme vsebino sporočila SMS v tekstovni obliki in izvede transformacijo XSLT, v kateri je definirana transformacijska predloga WTX. Rezultat transformacije je sporočilo XML.



Slika 4-27: Primer vhodnega sporočila SMS in izhodnega sporočila XML

Drugo pravilo v primeru napake pri procesiranju zahtevka vrne uporabniku prijazno sporočilo o napaki.



Slika 4-28: Primer napake pri izvajanju transformacijske predloge WTX

Ob uporabi pomožne storitve binarne transformacije zahtevek ne zapusti naprave DataPower, zato smo pri nastavitvah zalednega sistema uporabili povratno zanko.

4.5.3.2 Storitev časovnega žigosanja

Storitev smo pripravili z uporabo storitve XMLF. Poslušalca smo nastavili, da posluša na vseh vhodnih vmesnikih (IP naslov 0.0.0.0) in vratih 3002. Vsak zahtevek, ki na napravo DataPower vstopi na vratih 3002, se procesira v tej storitvi.

V politiki obdelave zahtevkov smo definirali dve pravili: prvo pravilo v smeri klient – strežnik - klient in drugo, ki se sproži v primeru napak ob procesiranju zahtevkov.

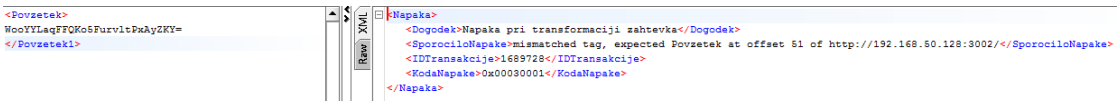
Configured Rules				
Order	**Rule Name**	**Direction**	**Actions**	
	TimeStampService_policy_rule_0	**Both Direction**		delete rule
	TimeStampService_policy_rule_1	Error		delete rule

Slika 4-29: Politika obdelave zahtevkov za časovno žigosanje

Prvo pravilo sprejme povzetek sporočila XML, ovitega z elementom XML, in izvede transformacijo XSLT, v kateri se povzetku doda časovni žig (podrobnosti so opisane v poglavju 4.5.2.1). Naslednji korak procesiranja je izvedba digitalnega podpisovanja dokumenta z uporabo samopodpisanega digitalnega potrdila. Uporabljeni algoritmi so RSA za podpisovanje in SHA-1 za povzetke. Pravilo vrne digitalno podpisano in časovno ožigosano sporočilo XML.

Slika 4-30: Primer časovnega žigosanja povzetka sporočila XML

Drugo pravilo v primeru napake pri procesiranju zahtevka vrne uporabniku prijazno sporočilo o napaki.



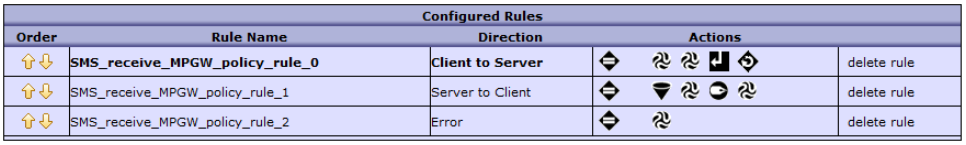
Slika 4-31: Primer napake pri časovnem žigosanju

Ob uporabi pomožne storitve časovnega žigosanja zahtevek ne zapusti naprave DataPower, zato smo pri nastavitvah zalednega sistema uporabili povratno zanko.

4.5.3.3 Storitev transformacije sporočil SMS v digitalno podpisana, časovno overovljena sporočila XML

Krovno storitev smo pripravili z uporabo MPGW storitve. Poslušalca smo nastavili, da posluša na vseh vhodnih vmesnikih (IP naslov 0.0.0.0) in vratih 80. To so privzeta vrata protokola HTTP.

V politiki obdelave zahtevkov smo definirali tri pravila: prvo pravilo v smeri klient – strežnik, drugo pravilo v smeri strežnik – klient in tretje, ki se sproži v primeru napak ob procesiranju zahtevkov.



Slika 4-32: Politika obdelave zahtevkov krovne storitve

Prvo pravilo sprejme zahtevek, ki ga posreduje aplikacija SMS Gateway. Zahtevek pride v obliki poizvedbe URL s parametri. Prva transformacija XSLT spremeni parametre URL v format XML. Druga transformacija XSLT izvleče metapodatke (telefonsko številko pošiljatelja) in jih shrani v kontekst transakcije. Kontekst transakcije se uporablja, kadar želimo prenesti informacije iz enega koraka procesiranja v drug korak (recimo vrednost spremenljivke). Transformacija kot rezultat vrne izvlečeno vsebino sporočila SMS v obliki niza tekstovnih podatkov. Ta niz naprava DataPower pošlje na pomožno storitev za transformacijo sporočil SMS v sporočila XML. Za zaledni sistem smo tako nastavili interni naslov 127.0.0.1 in vrata 3000.

Drugo pravilo zahtevke najprej filtrira – v primeru napake pri procesiranju v pomožni storitvi filter ustavi procesiranje pravila in zahtevek preusmeri na tretje pravilo. Drugi korak v pravilu je izdelava povzetka sporočila XML, pošiljanje povzetka na pomožno storitev za časovno žigosanje in ovijanje sporočila XML z ovojnico SOAP. V tretjem koraku se vrši digitalno podpisovanje zahtevka SOAP po standardu WSSec. Zadnji korak v pravilu je pošiljanje sporočila SMS pošiljatelju. Transformacija XSLT sestavi naslov URL – telefonsko številko pošiljatelja vzame iz konteksta transakcije, vsebino sporočila pa iz spremenljivke – in pokliče DataPower funkcijo open-url(), ki zahtevek pošlje preko protokola HTTP GET na SMS Gateway aplikacijo.

Tretje pravilo v primeru napake pri procesiranju zahtevka v krovni storitvi ali v kateri izmed pomožnih storitev vrne uporabniku prijazno sporočilo o napaki.

4.6 Testiranje sistema

Razvoj testnega sistema smo želeli prilagoditi na način, da bo testiranje delovanja posameznih delov rešitve možno, še preden bo celoten sistem dokončan. Testiranje posameznih delov sistema se torej lahko izvede ločeno.

Pošiljanje sporočil SMS smo testirali z uporabo internetnih strani, ki ponujajo brezplačno pošiljanje sporočil SMS. Na takšni strani smo vnesli telefonsko številko mobilne naprave z nameščeno aplikacijo SMS Gateway in sporočilo SMS, ki je ustrezalo definiranemu formatu.

Testiranje transformacije WTX smo najprej opravili v orodju WTX, nato pa na napravi DataPower. Pomožno storitev smo klicali s pomočjo orodja cURL, ki omogoča pošiljanje binarnih datotek in s pomočjo orodja SOAP UI.

Primer pošiljanja tekstovne datoteke na pomožno storitev:

```
curl --data-binary @..\..\testni_primer_1.txt http://192.168.50.128:3000
```

Testiranje storitve TSA smo izvedli s pomočjo orodja SOAP UI. Orodje omogoča pošiljanje zahtevkov na definiran naslov in pregled odgovorov.

Testiranje pošiljanja sporočil SMS smo izvedli s pomočjo brskalnika Mozilla Firefox in razširitve brskalnika HttpRequester. Orodje HttpRequester ponuja pošiljanje zahtevkov preko različnih metod HTTP (Get, Post, Put). V orodju smo vnesli primerno sestavljen URL naslov mobilne naprave z nameščeno SMS Gateway aplikacijo in vrata, na katerih aplikacija posluša, ter pregledovali odzive aplikacije.

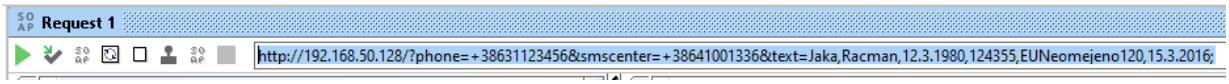
Razvita rešitev je v osnovi namenjena prejemanju sporočil SMS, a jo je možno testirati preko različnih kanalov. Za celovito testiranje smo izbrali testiranje s pomočjo orodja SOAP UI, ki najbolj pregledno vrne odgovor.

4.6.1 Pošiljanje testnega zahtevka

Aplikacija SMS Gateway posreduje sporočilo SMS v obliki parametrizirane poizvedbe URL. Posredovanje sporočila SMS smo simulirali v orodju SOAP UI s klicem takšne poizvedbe na napravo DataPower.

Simuliran parametriziran naslov URL izgleda takole:

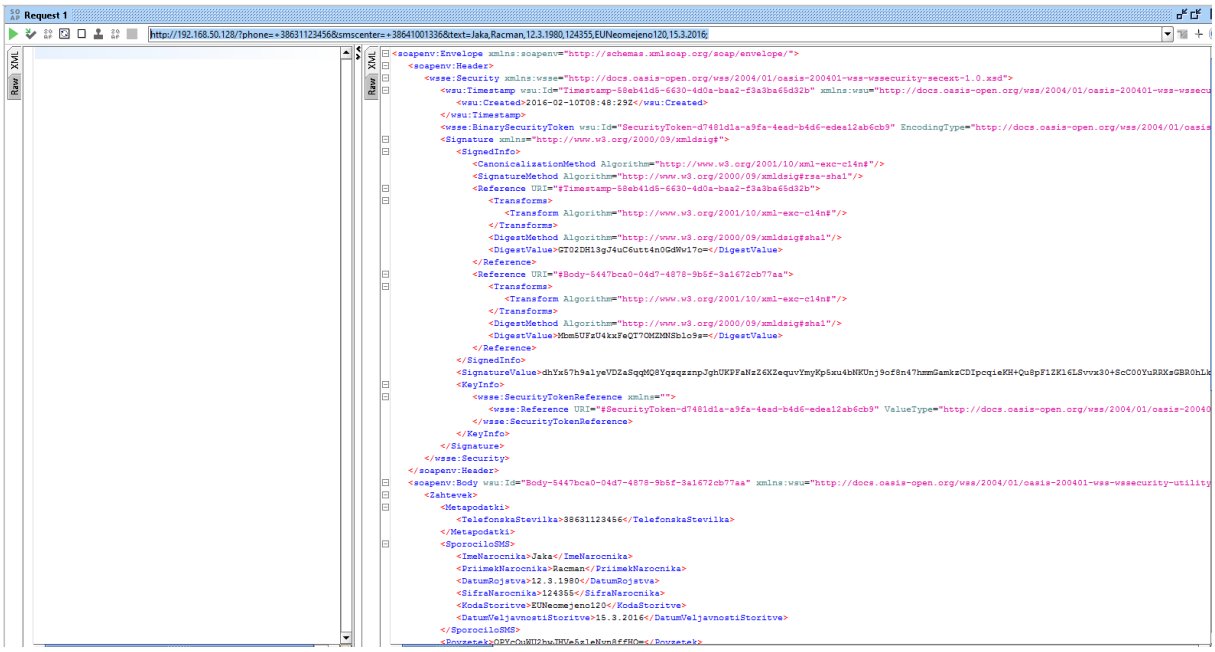
http://<naslov_DataPower_naprave>:<vrata_MPGW_storitve>/?phone=<telefonska_stevilka_posiljatelja_v_polni_obliki>&smscenter=<stevilka_SMS-SC>>&text=<vsebina_sporocila_SMS_v_definirani_obliki>



Slika 4-33: Primer parametrizirane URL poizvedbe za simulacijo sporočila SMS

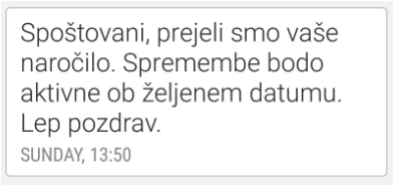
4.6.2 Odgovor testnega sistema

Razvita rešitev v primeru pravilnega klica vrne digitalno podpisano in časovno overovljeno sporočilo XML.



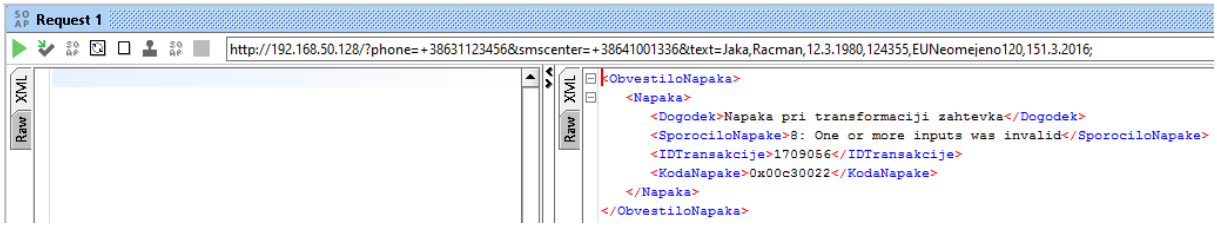
Slika 4-34: Primer digitalno podpisanega in časovno overovljenga sporočila XML

Pošiljatelj sporočila SMS ob uspešnem procesiranju zahtevka v odgovor dobi sporočilo SMS.



Slika 4-35: Primer prejetega sporočila SMS na mobilnem telefonu

V primeru napačnega klica ali napake v procesiranju zahtevka sistem vrne uporabniku prijazno obvestilo o napaki. Prilagamo primer napačnega sporočila SMS – željeni datum aktivacije storitve je v napačnem formatu.



Slika 4-36: Primer napačnega sporočila SMS

Poglavje 5 Zaključek

V diplomski nalogi smo razvili sistem za transformacijo sporočil SMS v digitalno podpisana in časovno overovljena sporočila XML, ki so po slovenski zakonodaji in e-SLOG priporočilih primerna za kratkoročno hranjenje v elektronskih arhivih. Sistem smo zasnovali za izmenjavo podatkov z e-arhivskim sistemom preko spletnih storitev in SOAP protokola.

Ob resni uporabi sistema bi morali vpeljati tudi sistem hranjenja digitalnih potrdil in preverjanja veljavnosti tako samih digitalnih potrdil kot tudi celotne verige overiteljev, vključno z vsemi pogoji za ustrezno infrastrukturo, vpeljavo predpisanih poslovnih procesov in usposobljenost zaposlenih. Dodatna komponenta sistema je postavitev in uporaba elektronskega arhiva.

Na podlagi uporabe razvitega sistema bi lahko mobilni operaterji obogatili sicer že obstoječ komunikacijski kanal (sporočila SMS) za upravljanje poslovnih procesov in pospešili svoje poslovne procese v zadovoljstvo naročnikov.

Glavne komponente sistema so razvite z namenskimi komercialnimi orodji, ki zagotavljajo podporo svetovnim standardom, visoko zmogljivost in uporabniško podporo. Sistem je zelo prilagodljiv in se ga z manjšimi spremembami lahko hitro prične uporabljati v resne poslovne namene.

Uporaba takšnega sistema sicer lahko pospeši poslovne procese, ne odpravlja pa zakonske potrebe po lastnoročnemu podpisu pogodbe ali aneksa k pogodbi. Za to bi moral sistem kratkih sporočil SMS omogočati podpis sporočila z uporabnikovim osebnim digitalnim potrdilom, nameščenim na mobilni napravi. Da bi uporabnikom zagotovili elektronsko storitev, enakovredno papirnemu poslovanju, bi morali razviti mobilno aplikacijo, ki bi posredovala sporočila, podpisana z uporabnikovim kvalificiranim osebnim digitalnim potrdilom. S tem uporabnike omejimo na uporabo pametnih telefonov, izkoriščanje prenosa podatkov ali povezave z internetom in povečamo možnost izgube identitete ob izgubi ali kraji mobilne naprave zaradi na napravi nameščenega osebnega digitalnega potrdila.

Tekom razvoja informacijske rešitve smo prepoznali nekaj področij, kjer bi lahko izboljšali oziroma spremenili delovanje sistema.

V transformaciji WTX bi lahko vpeljali boljše in obširnejše preverjanje pravilnosti podatkov. Vpeljali bi lahko seznam možnih storitev, s pomočjo katerega bi preverjali vnos podatkov in zavračali zahtevke z napačno kodo storitve. Na podlagi tega seznama bi tudi avtomatizirali nadaljnje korake obravnave in glede na kodo storitve sprožali različne poslovne procese v informacijskih sistemih mobilnega operaterja.

Napravo DataPower bi lahko povezali z repozitorijem telefonskih številk mobilnega operaterja in v procesu obogatitve sporočila XML dodali več metapodatkov o naročniku za potrebe ostalih informacijskih sistemov (na primer MSISDN številko, ID naročnika ...).

S povezavo z repozitorijem bi lahko vpeljali tudi predhodno razpoznavo naročnika. Na napravi DataPower bi ob prejemu zahtevka izvedli akcijo »AAA«, v kateri bi določili, da lahko procesiranje nadaljujejo samo zahtevki, ki so bili poslani s strani pravih naročnikov. V tej akciji bi tudi lahko določili, kako pogosto se lahko prejemajo zahteve s strani posameznega naročnika, in s tem zaščitili sisteme pred preobremenitvami (DoS napadi).

V sistem bi morali vpeljati še revizijsko sled za vse aktivnosti – tako sistemske kot človeške.

Literatura

[1] Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivov (ZVDAGA). (2006). Uradni list RS, št.30/06. [Online]. Dosegljivo: http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4284

[2] Uredba o varstvu dokumentarnega in arhivskega gradiva. (2006). Uradni list RS, št.86/06. [Online]. Dosegljivo: http://www.pisrs.si/Pis.web/pregledPredpisa?id=URED3462

[3] Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP). (2000). Uradni list RS, št. 98/04. [Online]. Dosegljivo: http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1973

[4] Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje. (2000). Uradni list RS, št. 77/00. [Online]. Dosegljivo: http://www.pisrs.si/Pis.web/pregledPredpisa?id=URED1148

[5] Projekt e-SLOG: Priporočila za format dokumenta (XML) za varen e-podpis; Priporočila uporabe kriptografskih algoritmov, v1.0. (2004). [Online]. Dosegljivo: https://www.gzs.si/e-poslovanje/dokumentacija/e-SLOG_Priporocila_za%20format_dokumenta_in_uporabe_kriptografskih_algoritmov_1.0.pdf

[6] Projekt e-SLOG: Tehnično priporočilo za varno elektronsko arhiviranje, v0.99. (2003). [Online]. Dosegljivo: https://www.gzs.si/e-poslovanje/dokumentacija/eSLOG-Elektronski_arhiv_0.99%28v_pripravi%29.pdf

[7] Bergland, J. Et al. (2009). Integrating Systems Through Universal Transformation Using IBM WebSphere Transformation Extender. ITSO

[8] Detailed System Requirements for Transformation Extender (17.3.2015). [Online]. Dosegljivo: http://www-01.ibm.com/support/docview.wss?uid=swg27043907

[9] Kapadia, S. (2012). Strategic Overview of WebSphere Appliances. ITS

[10] XML appliance (julij 2011). Wikipedija The Free Encyclopedia. [Online]. Dosegljivo: https://en.wikipedia.org/wiki/XML_appliance

[11] OpenSSL: Cryptography and SSL/TLS Toolkit (2016). [Online]. Dosegljivo: https://www.openssl.org/

[12] OpenSSL for Windows (2016). [Online]. Dosegljivo: http://gnuwin32.sourceforge.net/packages/openssl.htm

[13] cURL (2016). [Online]. Dosegljivo: https://curl.haxx.se/

[14] SoapUI by SmartBear (2016). [Online]. Dosegljivo: https://www.soapui.org/

[15] Google Play: SMS Gateway by b00lean (2016). [Online]. Dosegljivo: https://play.google.com/store/apps/details?id=eu.apksoft.android.smsgateway&hl=en

[16] Wilde, E., Vaha-Sipila, A. (2010). URI Scheme for Global System for Mobile Communications (GSM) Short Message Service (SMS). [Online]. Dosegljivo: https://www.ietf.org/rfc/rfc5724.txt

[17] Osnove varnih časovnih žigov (2016). [Online]. Dosegljivo: http://www.si-tsa.si/osnove.php

[18] Storitev NTP (2016). [Online]. Dosegljivo: https://www.arnes.si/storitve/omrezne-storitve/storitev-ntp/

[19] Uporaba kriptografije v internetu (marec 2006). [Online]. Dosegljivo: http://www.si-ca.si/kripto/kr-podp.htm

[20] Short Message Service (julij 2008). Wikipedija The Free Encyclopedia. [Online]. Dosegljivo: https://en.wikipedia.org/wiki/Short_Message_Service

[21] Trusted Timestamping (avgust 2012). Wikipedija The Free Encyclopedia. [Online]. Dosegljivo: https://en.wikipedia.org/wiki/Trusted_timestamping